



System Administration Guide: IP Services

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 816-4554-10
January 2005

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, et Solaris sont des marques de fabrique ou des marques déposées, de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



041208@10536



Contents

Preface 27

Part I Introducing System Administration: IP Services 33

1 Fundamentals of TCP/IP (Overview) 35

Introducing the Internet Protocol Suite 35

 Protocol Layers and the Open Systems Interconnection Model 36

 TCP/IP Protocol Architecture Model 37

How the TCP/IP Protocols Handle Data Communications 43

 Data Encapsulation and the TCP/IP Protocol Stack 43

 TCP/IP Internal Trace Support 47

Finding Out More About TCP/IP and the Internet 47

 Computer Books About TCP/IP 47

 TCP/IP and Networking Related Web Sites 47

 Requests for Comments and Internet Drafts 48

Part II TCP/IP Administration 49

2 Planning Your TCP/IP Network (Tasks) 51

Network Planning (Task Map) 52

Determining the Network Hardware 53

Deciding on an IP Addressing Format for Your Network 54

 IPv4 Addresses 54

 IPv4 Addresses in CIDR Format 55

 DHCP Addresses 55

IPv6 Addresses	55
Private Addresses and Documentation Prefixes	55
Obtaining Your Network's IP Number	56
Designing an IPv4 Addressing Scheme	57
Designing Your IPv4 Addressing Scheme	58
IPv4 Subnet Number	59
Designing Your CIDR IPv4 Addressing Scheme	59
Using Private IPv4 Addresses	60
How IP Addresses Apply to Network Interfaces	61
Naming Entities on Your Network	62
Administering Host Names	62
Selecting a Name Service and Directory Service	62
Adding Routers to Your Network	64
Network Topology Overview	65
How Routers Transfer Packets	66
3 Introducing IPv6 (Overview)	69
Major Features of IPv6	69
Expanded Addressing	70
Address Autoconfiguration and Neighbor Discovery	70
Header Format Simplification	70
Improved Support for IP Header Options	70
Application Support for IPv6 Addressing	70
Additional IPv6 Resources	71
IPv6 Network Overview	72
IPv6 Addressing Overview	74
Parts of the IPv6 Address	75
Abbreviating IPv6 Addresses	76
Prefixes in IPv6	76
Unicast Addresses	77
Multicast Addresses	80
Anycast Addresses and Groups	80
IPv6 Neighbor Discovery Protocol Overview	81
IPv6 Address Autoconfiguration	82
Stateless Autoconfiguration Overview	82
Overview of IPv6 Tunnels	83

4	Planning an IPv6 Network (Tasks)	85
	IPv6 Planning (Task Maps)	85
	IPv6 Network Topology Scenario	87
	Preparing the Existing Network to Support IPv6	88
	Preparing the Network Topology for IPv6 Support	89
	Preparing Network Services for IPv6 Support	89
	Preparing Servers for IPv6 Support	90
	▼ How to Prepare Network Services for IPv6 Support	90
	▼ How to Prepare DNS for IPv6 Support	91
	Planning for Tunnels in the Network Topology	91
	Security Considerations for the IPv6 Implementation	92
	Preparing an IPv6 Addressing Plan	92
	Obtaining a Site Prefix	93
	Creating the IPv6 Numbering Scheme	93
5	Configuring TCP/IP Network Services and IPv4 Addressing (Tasks)	95
	Before You Configure an IPv4 Network (Task Map)	96
	Determining Host Configuration Modes	97
	Systems That Should Run in Local Files Mode	97
	Systems That Are Network Clients	98
	Mixed Configurations	98
	IPv4 Network Topology Scenario	99
	Adding a Subnet to a Network (Task Map)	99
	Network Configuration Task Map	101
	Network Configuration Procedures	101
	▼ How to Configure a Host for Local Files Mode	102
	▼ How to Set Up a Network Configuration Server	104
	Configuring Network Clients	105
	▼ How to Configure Hosts for Network Client Mode	105
	▼ How to Enable Static Routing on a Network Client	106
	▼ How to Enable Dynamic Routing on a Network Client	107
	Monitoring and Modifying Transport Layer Services	108
	▼ How to Log the IP Addresses of All Incoming TCP Connections	108
	▼ How to Add Services That Use the SCTP Protocol	109
	▼ How to Use TCP Wrappers to Control Access to TCP Services	112
	Administering Physical Interfaces	112
	Administering the Physical Interface	113
	▼ How to Add a Physical Interface After Installation	113

▼ How to Remove a Physical Interface	115
Configuring VLANs	115
▼ How To Configure Static VLANs	116
Configuring a Router	118
▼ How to Configure an IPv4 Router	119
Multihomed Hosts	121
▼ How to Create a Multihomed Host	121
6 Configuring an IPv6 Network (Tasks)	123
General IPv6 Network Configuration Tasks (Task Map)	123
Prerequisites for Configuring IPv6 on the Network	125
Configuring an IPv6 Router	125
▼ How to Configure an IPv6–Enabled Router	126
▼ How to Manually Configure Interfaces for IPv6	128
Tasks for Configuring Tunnels for IPv6 Support (Task Map)	129
Configuring Tunnels for IPv6 Support	130
▼ How to Manually Configure IPv6 Over IPv4 Tunnels	130
▼ How to Manually Configure IPv6 Over IPv6 Tunnels	131
▼ How to Configure IPv4 Over IPv6 Tunnels	132
▼ How to Configure a 6to4 Tunnel	133
▼ How to Configure a 6to4 Tunnel to a 6to4 Relay Router	136
Configuring Name Service Support for IPv6	138
▼ How to Add IPv6 Addresses to DNS	138
Adding IPv6 Addresses to NIS	139
▼ How to Display IPv6 Name Service Information	139
▼ How to Verify That DNS IPv6 PTR Records Are Updated Correctly	140
▼ How to Display IPv6 Information Through NIS	141
▼ How to Display IPv6 Information Independent of the Name Service	141
Configuring IPv6 on a Host	142
▼ How to Enable IPv6 Address Autoconfiguration	142
Using Temporary Addresses for an Interface	144
▼ How to Configure a Temporary Address	144
Configuring IPv6 on Servers	147
▼ How to Manually Configure a Link-Local Address	147
7 Administering a TCP/IP Network (Tasks)	151
Major TCP/IP Administrative Tasks (Task Map)	152

Monitoring the Interface Configuration With the <code>ifconfig</code> Command	153
▼ How to Get Information About a Specific Interface	153
▼ How to Display Interface Address Assignments	155
Monitoring Network Status With the <code>netstat</code> Command	157
▼ How to Display Statistics by Protocol	157
▼ How to Display the Status of Transport Protocols	159
▼ How to Display Network Interface Status	160
▼ How to Display the Status of Sockets	160
▼ How to Display the Status of Transmissions for Packets of a Specific Address Type	162
▼ How to Display the Status of Known Routes	163
Probing Remote Hosts With the <code>ping</code> Command	164
▼ How to Determine if a Remote Host Is Running	164
▼ How to Determine if a Host Is Dropping Packets	164
Administering and Logging Network Status Displays	165
▼ How to Control the Display Output of IP-Related Commands	165
▼ How to Log Actions of the IPv4 Routing Daemon	166
▼ How to Trace the Activities of the IPv6 Neighbor Discovery Daemon	167
Displaying Routing Information With the <code>traceroute</code> Command	168
▼ How to Find Out the Route to a Remote Host	169
▼ How to Trace All Routes	169
Monitoring Packet Transfers With the <code>snoop</code> Command	170
▼ How to Check Packets From All Interfaces	170
▼ How to Capture <code>snoop</code> Output Into a File	171
▼ How to Check Packets Between an IPv4 Server and a Client	172
▼ How to Monitor IPv6 Network Traffic	173
Administering Default Address Selection	173
▼ How to Administer the IPv6 Address Selection Policy Table	174
▼ How to Modify the IPv6 Address Selection Table for the Current Session Only	175
8 Troubleshooting Network Problems (Tasks)	177
General Network Troubleshooting Tips	177
Running Basic Diagnostic Checks	177
▼ How to Perform Basic Network Software Checking	178
Common Problems When Deploying IPv6	179
IPv4 Router Cannot Be Upgraded to IPv6	179
Problems After Upgrading Services to IPv6	179

Current ISP Does Not Support IPv6	179
Security Issues When Tunneling to a 6to4 Relay Router	180
Known Issues With a 6to4 Router	180

9 TCP/IP and IPv4 in Depth (Reference) 183

TCP/IP Configuration Files	183
/etc/hostname. <i>interface</i> File	184
/etc/nodename File	184
/etc/defaultdomain File	185
/etc/defaultrouter File	185
hosts Database	185
netmasks Database	188
inetd Internet Services Daemon	192
Network Databases and the nsswitch.conf File	192
How Name Services Affect Network Databases	193
nsswitch.conf File	195
bootparams Database	197
ethers Database	198
Other Network Databases	199
protocols Database	200
services Database	200
Routing Protocols in the Solaris OS	201
Routing Information Protocol (RIP)	201
ICMP Router Discovery (RDISC) Protocol	201
Network Classes	202
Class A Network Numbers	202
Class B Network Numbers	203
Class C Network Numbers	203

10 IPv6 in Depth (Reference) 205

IPv6 Addressing Formats Beyond the Basics	205
6to4-Derived Addresses	206
IPv6 Multicast Addresses in Depth	207
IPv6 Packet Header Format	208
IPv6 Extension Headers	210
Dual-Stack Protocols	210
Solaris 10 IPv6 Implementation	211

IPv6 Configuration Files	211
IPv6-Related Commands	216
IPv6-Related Daemons	222
IPv6 Neighbor Discovery Protocol	226
ICMP Messages From Neighbor Discovery	226
Autoconfiguration Process	227
Neighbor Solicitation and Unreachability	229
Duplicate Address Detection Algorithm	229
Proxy Advertisements	229
Inbound Load Balancing	230
Link-Local Address Change	230
Comparison of Neighbor Discovery to ARP and Related IPv4 Protocols	230
IPv6 Routing	232
Router Advertisement	232
IPv6 Tunnels	233
Configured Tunnels	235
6to4 Automatic Tunnels	237
IPv6 Extensions to Solaris Name Services	241
ipnodes Database	241
DNS Extensions for IPv6	242
NIS Extensions for IPv6	242
Changes to the <code>nsswitch.conf</code> File	242
Changes to Name Service Commands	243
NFS and RPC IPv6 Support	244
IPv6 Over ATM Support	244

Part III DHCP 245

11 About Solaris DHCP (Overview)	247
About the DHCP Protocol	247
Advantages of Using Solaris DHCP	248
How DHCP Works	249
Solaris DHCP Server	252
DHCP Server Management	253
DHCP Data Store	253
DHCP Manager	255
DHCP Command-Line Utilities	255

	Role-Based Access Control for DHCP Commands	256
	DHCP Server Configuration	257
	IP Address Allocation	257
	Network Configuration Information	258
	About DHCP Options	258
	About DHCP Macros	259
	Solaris DHCP Client	261
12	Planning for DHCP Service (Tasks)	263
	Preparing Your Network for the DHCP Service (Task Map)	263
	Mapping Your Network Topology	264
	Determining the Number of DHCP Servers	265
	Updating System Files and Netmask Tables	266
	Making Decisions for Your DHCP Server Configuration (Task Map)	268
	Selecting a Host to Run the DHCP Service	268
	Choosing the DHCP Data Store	269
	Setting a Lease Policy	269
	Determining Routers for DHCP Clients	270
	Making Decisions for IP Address Management (Task Map)	271
	Number and Ranges of IP Addresses	272
	Client Host Name Generation	272
	Default Client Configuration Macros	272
	Dynamic and Permanent Lease Types	273
	Reserved IP Addresses and Lease Type	274
	Planning for Multiple DHCP Servers	274
	Planning DHCP Configuration of Your Remote Networks	275
	Selecting the Tool for Configuring DHCP	276
	DHCP Manager Features	276
	dhcpconfig Features	276
	Comparison of DHCP Manager and dhcpconfig	277
13	Configuring the DHCP Service (Tasks)	279
	Configuring and Unconfiguring a DHCP Server Using DHCP Manager	279
	Configuring DHCP Servers	280
	▼ How to Configure a DHCP Server (DHCP Manager)	282
	Configuring BOOTP Relay Agents	283
	▼ How to Configure a BOOTP Relay Agent (DHCP Manager)	284

	Unconfiguring DHCP Servers and BOOTP Relay Agents	285
	DHCP Data on an Unconfigured Server	285
	▼ How to Unconfigure a DHCP Server or a BOOTP Relay Agent (DHCP Manager)	286
	Configuring and Unconfiguring a DHCP Server Using <code>dhcpconfig</code> Commands	287
	▼ How to Configure a DHCP Server (<code>dhcpconfig -D</code>)	287
	▼ How to Configure a BOOTP Relay Agent (<code>dhcpconfig -R</code>)	288
	▼ How to Unconfigure a DHCP Server or a BOOTP Relay Agent (<code>dhcpconfig -U</code>)	288
14	Administering DHCP (Tasks)	291
	About DHCP Manager	292
	DHCP Manager Window	292
	DHCP Manager Menus	293
	Starting and Stopping DHCP Manager	294
	▼ How to Start and Stop DHCP Manager	294
	Setting Up User Access to DHCP Commands	295
	▼ How to Grant Users Access to DHCP Commands	295
	Starting and Stopping the DHCP Service	296
	▼ How to Start and Stop the DHCP Service (DHCP Manager)	297
	▼ How to Enable and Disable the DHCP Service (DHCP Manager)	297
	▼ How to Enable and Disable the DHCP Service (<code>dhcpconfig -S</code>)	297
	DHCP Service and the Service Management Facility	298
	Modifying DHCP Service Options (Task Map)	299
	Changing DHCP Logging Options	301
	▼ How to Generate Verbose DHCP Log Messages (DHCP Manager)	302
	▼ How to Generate Verbose DHCP Log Messages (Command Line)	303
	▼ How to Enable and Disable DHCP Transaction Logging (DHCP Manager)	303
	▼ How to Enable and Disable DHCP Transaction Logging (Command Line)	304
	▼ How to Log DHCP Transactions to a Separate <code>syslog</code> File	305
	Enabling Dynamic DNS Updates by a DHCP Server	305
	▼ How to Enable Dynamic DNS Updating for DHCP Clients	306
	Client Host Name Registration	308
	Customizing Performance Options for the DHCP Server	309
	▼ How to Customize DHCP Performance Options (DHCP Manager)	310
	▼ How to Customize DHCP Performance Options (Command Line)	310
	Adding, Modifying, and Removing DHCP Networks (Task Map)	311

Specifying Network Interfaces for DHCP Monitoring	312
▼ How to Specify Network Interfaces for DHCP Monitoring (DHCP Manager)	313
▼ How to Specify Network Interfaces for DHCP Monitoring (dhcpconfig)	314
Adding DHCP Networks	314
▼ How to Add a DHCP Network (DHCP Manager)	315
▼ How to Add a DHCP Network (dhcpconfig)	316
Modifying DHCP Network Configurations	317
▼ How to Modify the Configuration of a DHCP Network (DHCP Manager)	317
▼ How to Modify the Configuration of a DHCP Network (dhtadm)	318
Removing DHCP Networks	319
▼ How to Remove a DHCP Network (DHCP Manager)	320
▼ How to Remove a DHCP Network (pntadm)	320
Supporting BOOTP Clients With the DHCP Service (Task Map)	321
▼ How to Set Up Support of Any BOOTP Client (DHCP Manager)	322
▼ How to Set Up Support of Registered BOOTP Clients (DHCP Manager)	323
Working With IP Addresses in the DHCP Service (Task Map)	324
Adding IP Addresses to the DHCP Service	328
▼ How to Add a Single IP Address (DHCP Manager)	330
▼ How to Duplicate an Existing IP Address (DHCP Manager)	330
▼ How to Add Multiple IP Addresses (DHCP Manager)	331
▼ How to Add IP Addresses (pntadm)	331
Modifying IP Addresses in the DHCP Service	332
▼ How to Modify IP Address Properties (DHCP Manager)	333
▼ How to Modify IP Address Properties (pntadm)	334
Removing IP Addresses From the DHCP Service	334
Marking IP Addresses as Unusable by the DHCP Service	334
▼ How to Mark IP Addresses as Unusable (DHCP Manager)	335
▼ How to Mark IP Addresses as Unusable (pntadm)	335
Deleting IP Addresses From the DHCP Service	336
▼ How to Delete IP Addresses From DHCP Service (DHCP Manager)	336
▼ How to Delete IP Addresses From the DHCP Service (pntadm)	337
Assigning a Reserved IP Address to a DHCP Client	337
▼ How to Assign a Consistent IP Address to a DHCP Client (DHCP Manager)	338
▼ How to Assign a Consistent IP Address to a DHCP Client (pntadm)	339
Working With DHCP Macros (Task Map)	340
▼ How to View Macros Defined on a DHCP Server (DHCP Manager)	341

▼ How to View Macros Defined on a DHCP Server (dhtadm)	342
Modifying DHCP Macros	342
▼ How to Change Values for Options in a DHCP Macro (DHCP Manager)	343
▼ How to Change Values for Options in a DHCP Macro (dhtadm)	344
▼ How to Add Options to a DHCP Macro (DHCP Manager)	344
▼ How to Add Options to a DHCP Macro (dhtadm)	345
▼ How to Delete Options From a DHCP Macro (DHCP Manager)	345
▼ How to Delete Options From a DHCP Macro (dhtadm)	346
Creating DHCP Macros	346
▼ How to Create a DHCP Macro (DHCP Manager)	347
▼ How to Create a DHCP Macro (dhtadm)	348
Deleting DHCP Macros	349
▼ How to Delete a DHCP Macro (DHCP Manager)	349
▼ How to Delete a DHCP Macro (dhtadm)	349
Working With DHCP Options (Task Map)	350
Creating DHCP Options	353
▼ How to Create DHCP Options (DHCP Manager)	354
▼ How to Create DHCP Options (dhtadm)	355
Modifying DHCP Options	356
▼ How to Modify DHCP Option Properties (DHCP Manager)	356
▼ How to Modify DHCP Option Properties (dhtadm)	357
Deleting DHCP Options	358
▼ How to Delete DHCP Options (DHCP Manager)	358
▼ How to Delete DHCP Options (dhtadm)	359
Modifying the Solaris DHCP Client's Option Information	359
Supporting Solaris Network Installation With the DHCP Service	360
Supporting Remote Boot and Diskless Boot Clients (Task Map)	361
Setting Up DHCP Clients to Receive Information Only (Task Map)	362
Converting to a New DHCP Data Store	363
▼ How to Convert the DHCP Data Store (DHCP Manager)	364
▼ How to Convert the DHCP Data Store (dhcpconfig -C)	365
Moving Configuration Data Between DHCP Servers (Task Map)	365
▼ How to Export Data From a DHCP Server (DHCP Manager)	367
▼ How to Export Data From a DHCP Server (dhcpconfig -X)	368
▼ How to Import Data on a DHCP Server (DHCP Manager)	369
▼ How to Import Data on a DHCP Server (dhcpconfig -I)	369
▼ How to Modify Imported DHCP Data (DHCP Manager)	370
▼ How to Modify Imported DHCP Data (pntadm, dhtadm)	370

15	Configuring and Administering the DHCP Client	373
	About the Solaris DHCP Client	373
	DHCP Client Startup	374
	How the DHCP Client Manages Network Configuration Information	374
	DHCP Client Shutdown	375
	Enabling and Disabling a Solaris DHCP Client	375
	▼ How to Enable the Solaris DHCP Client	375
	▼ How to Disable a Solaris DHCP Client	376
	DHCP Client Administration	377
	ifconfig Command Options Used With the DHCP Client	377
	Setting DHCP Client Configuration Parameters	378
	DHCP Client Systems With Multiple Network Interfaces	379
	DHCP Client Host Names	380
	▼ How to Enable a Solaris Client to Request a Specific Host Name	380
	DHCP Client Systems and Name Services	381
	Setting Up DHCP Clients as NIS+ Clients	383
	▼ How to Set Up Solaris DHCP Clients as NIS+ Clients	383
	DHCP Client Event Scripts	386
16	Troubleshooting DHCP (Reference)	389
	Troubleshooting DHCP Server Problems	389
	NIS+ Problems and the DHCP Data Store	389
	IP Address Allocation Errors in DHCP	392
	Troubleshooting DHCP Client Configuration Problems	395
	Problems Communicating With the DHCP Server	396
	▼ How to Run the DHCP Client in Debugging Mode	396
	▼ How to Run the DHCP Server in Debugging Mode	397
	▼ How to Use snoop to Monitor DHCP Network Traffic	397
	Problems With Inaccurate DHCP Configuration Information	404
	Problems With the DHCP Client-Supplied Host Name	404
17	DHCP Commands and Files (Reference)	409
	DHCP Commands	409
	Running DHCP Commands in Scripts	410
	Files Used by the DHCP Service	416
	DHCP Option Information	418
	Determining if Your Site Is Affected	419

Differences Between dhcptags and inittab Files	419
Converting dhcptags Entries to inittab Entries	421

Part IV IP Security 423

18 IP Security Architecture (Overview)	425
Introduction to IPsec	425
IPsec RFCs	427
IPsec Terminology	427
IPsec Packet Flow	428
IPsec Security Associations	431
Key Management in IPsec	431
IPsec Protection Mechanisms	432
Authentication Header	432
Encapsulating Security Payload	432
Authentication and Encryption Algorithms in IPsec	433
IPsec Protection Policies	434
Transport and Tunnel Modes in IPsec	435
Virtual Private Networks and IPsec	436
IPsec and NAT Traversal	437
IPsec and SCTP	438
IPsec and Solaris Zones	439
IPsec Utilities and Files	439
Changes to IPsec for the Solaris 10 Release	440
19 Configuring IPsec (Tasks)	443
Configuring IPsec (Task Map)	443
Configuring IPsec	444
▼ How to Secure Traffic Between Two Systems With IPsec	445
▼ How to Secure a Web Server With IPsec	447
▼ How to Display IPsec Policies	449
▼ How to Set Up a VPN With IPsec Over IPv4	450
▼ How to Set Up a VPN With IPsec Over IPv6	456
▼ How to Generate Random Numbers on a Solaris System	460
▼ How to Manually Create IPsec Security Associations	461
▼ How to Verify That Packets Are Protected With IPsec	465
▼ How to Create a Role for Configuring Network Security	467

20	IP Security Architecture (Reference)	469
	ipsecconf Command	469
	ipsecinit.conf File	470
	Sample ipsecinit.conf File	470
	Security Considerations for ipsecinit.conf and ipsecconf	471
	ipsecalgs Command	472
	Security Associations Database for IPsec	472
	Utilities for Key Generation in IPsec	473
	Security Considerations for ipseckey	473
	IPsec Extensions to Other Utilities	474
	ifconfig Command and IPsec	474
	snoop Command and IPsec	475
21	Internet Key Exchange (Overview)	477
	Key Management With IKE	477
	IKE Key Negotiation	478
	IKE Key Terminology	478
	IKE Phase 1 Exchange	479
	IKE Phase 2 Exchange	479
	IKE Configuration Choices	480
	IKE With Preshared Keys	480
	IKE With Public Key Certificates	480
	IKE and Hardware Acceleration	481
	IKE and Hardware Storage	481
	IKE Utilities and Files	482
	Changes to IKE for the Solaris 10 Release	483
22	Configuring IKE (Tasks)	485
	Configuring IKE (Task Map)	485
	Configuring IKE With Preshared Keys (Task Map)	486
	Configuring IKE With Preshared Keys	487
	▼ How to Configure IKE With Preshared Keys	487
	▼ How to Refresh IKE Preshared Keys	490
	▼ How to Add an IKE Preshared Key for a New Policy Entry in ipsecinit.conf	491
	▼ How to Verify That IKE Preshared Keys Are Identical	494
	Configuring IKE With Public Key Certificates (Task Map)	496
	Configuring IKE With Public Key Certificates	496

▼ How to Configure IKE With Self-Signed Public Key Certificates	497
▼ How to Configure IKE With Certificates Signed by a CA	501
▼ How to Generate and Store Public Key Certificates on Hardware	506
▼ How to Handle a Certificate Revocation List	510
Configuring IKE for Mobile Systems (Task Map)	512
Configuring IKE for Mobile Systems	513
▼ How to Configure IKE for Off-Site Systems	513
Configuring IKE to Find Attached Hardware (Task Map)	520
Configuring IKE to Find Attached Hardware	520
▼ How to Configure IKE to Find the Sun Crypto Accelerator 1000 Board	521
▼ How to Configure IKE to Find the Sun Crypto Accelerator 4000 Board	522
Changing IKE Transmission Parameters (Task Map)	523
Changing IKE Transmission Parameters	524
▼ How to Change the Duration of Phase 1 IKE Key Negotiation	524
23 Internet Key Exchange (Reference)	527
IKE Daemon	527
IKE Policy File	528
IKE Administration Command	528
IKE Preshared Keys Files	529
IKE Public Key Databases and Commands	530
ikecert tokens Command	530
ikecert certlocal Command	530
ikecert certddb Command	531
ikecert certrldb Command	532
/etc/inet/ike/publickeys Directory	532
/etc/inet/secret/ike.privatekeys Directory	532
/etc/inet/ike/crls Directory	532
IKE Status and Error Messages	533
24 Solaris IP Filter (Overview)	535
Introduction to Solaris IP Filter	535
Information Sources for Open Source IP Filter	536
Guidelines for Using Solaris IP Filter	536
Using Solaris IP Filter Configuration Files	536
Working With Solaris IP Filter Rule Sets	537
Using Solaris IP Filter's Packet Filtering Feature	537

Using Solaris IP Filter's NAT Feature	540
Using Solaris IP Filter's Address Pools Feature	541
Activating Solaris IP Filter Using the <code>pf11</code> STREAMS Module	542
Solaris IP Filter Man Pages	543

25 Solaris IP Filter (Tasks) 545

Configuring Solaris IP Filter	545
▼ How to Enable Solaris IP Filter	546
▼ How to Re-Enable Solaris IP Filter	548
▼ How to Activate a NIC for Packet Filtering	549
Deactivating and Disabling Solaris IP Filter	550
▼ How to Deactivate Packet Filtering	551
▼ How to Deactivate NAT	552
▼ How to Deactivate Solaris IP Filter on a NIC	552
▼ How to Disable Packet Filtering	554
Working With Solaris IP Filter Rule Sets	554
Managing Packet Filtering Rule Sets for Solaris IP Filter	555
▼ How to View the Active Packet Filtering Rule Set	556
▼ How to View the Inactive Packet Filtering Rule Set	556
▼ How to Activate a Different Packet Filtering Rule Set	556
▼ How to Remove a Packet Filtering Rule Set	557
▼ How to Append Rules to the Active Packet Filtering Rule Set	558
▼ How to Append Rules to the Inactive Packet Filtering Rule Set	559
▼ How to Switch Between Active and Inactive Packet Filtering Rule Sets	559
▼ How to Remove an Inactive Packet Filtering Rule Set From the Kernel	560
Managing NAT Rules for Solaris IP Filter	561
▼ How to View Active NAT Rules	561
▼ How to Remove NAT Rules	562
▼ How to Append Rules to the NAT Rules	562
Managing Address Pools for Solaris IP Filter	563
▼ How to View Active Address Pools	563
▼ How to Remove an Address Pool	564
▼ How to Append Rules to an Address Pool	564
Displaying Statistics and Information for Solaris IP Filter	565
▼ How to View State Tables for Solaris IP Filter	566
▼ How to View State Statistics for Solaris IP Filter	567

▼ How to View NAT Statistics for Solaris IP Filter	567
▼ How to View Address Pool Statistics for Solaris IP Filter	568
▼ How to View <code>pfil</code> Statistics for Solaris IP Filter	568
Working With Log Files for Solaris IP Filter	569
▼ How to View Solaris IP Filter Log Files	569
▼ How to Flush the Packet Log File	570
▼ How to Save Logged Packets to a File	571
Creating and Editing Solaris IP Filter Configuration Files	572
▼ How to Create a Configuration File for Solaris IP Filter	572
Solaris IP Filter Configuration File Examples	573

Part V Mobile IP 579

26 Mobile IP (Overview)	581
Introduction to Mobile IP	581
Mobile IP Functional Entities	583
How Mobile IP Works	584
Agent Discovery	587
Agent Advertisement	587
Agent Solicitation	588
Care-of Addresses	588
Mobile IP With Reverse Tunneling	589
Limited Private Addresses Support	589
Mobile IP Registration	591
Network Access Identifier (NAI)	593
Mobile IP Message Authentication	593
Mobile Node Registration Request	593
Registration Reply Message	594
Foreign Agent Considerations	594
Home Agent Considerations	594
Dynamic Home Agent Discovery	595
Routing Datagrams to and From Mobile Nodes	595
Encapsulation Methods	595
Unicast Datagram Routing	596
Broadcast Datagrams	596
Multicast Datagram Routing	596
Security Considerations for Mobile IP	597

27	Administering Mobile IP (Tasks)	599
	Creating the Mobile IP Configuration File (Task Map)	599
	Creating the Mobile IP Configuration File	600
	▼ How to Plan for Mobile IP	600
	▼ How to Create the Mobile IP Configuration File	601
	▼ How to Configure the General Section	602
	▼ How to Configure the Advertisements Section	602
	▼ How to Configure the GlobalSecurityParameters Section	602
	▼ How to Configure the Pool Section	603
	▼ How to Configure the SPI Section	603
	▼ How to Configure the Address Section	603
	Modifying the Mobile IP Configuration File (Task Map)	605
	Modifying the Mobile IP Configuration File	606
	▼ How to Modify the General Section	606
	▼ How to Modify the Advertisements Section	606
	▼ How to Modify the GlobalSecurityParameters Section	607
	▼ How to Modify the Pool Section	608
	▼ How to Modify the SPI Section	608
	▼ How to Modify the Address Section	609
	▼ How to Add or Delete Configuration File Parameters	610
	▼ How to Display Current Parameter Values in the Configuration File	611
	Displaying Mobility Agent Status	612
	▼ How to Display Mobility Agent Status	613
	Displaying Mobility Routes on a Foreign Agent	614
	▼ How to Display Mobility Routes on a Foreign Agent	614
28	Mobile IP Files and Commands (Reference)	615
	Overview of the Solaris Mobile IP Implementation	615
	Mobile IP Configuration File	616
	Configuration File Format	617
	Sample Configuration Files	617
	Configuration File Sections and Labels	621
	Configuring the Mobility IP Agent	630
	Mobile IP Mobility Agent Status	631
	Mobile IP State Information	632

netstat Extensions for Mobile IP 632
snoop Extensions for Mobile IP 633

Part VI IPMP 635

- 29 Introducing IPMP (Overview) 637**
 - Why You Should Use IPMP 637
 - Solaris IPMP Components 638
 - IPMP Terminology and Concepts 638
 - Basic Requirements of IPMP 641
 - IPMP Addressing 642
 - Data Addresses 642
 - Test Addresses 642
 - Preventing Applications From Using Test Addresses 644
 - IPMP Interface Configurations 644
 - Standby Interfaces in an IPMP Group 644
 - Common IPMP Interface Configurations 645
 - IPMP Failure Detection and Recovery Features 646
 - Link-Based Failure Detection 646
 - Probe-Based Failure Detection 647
 - Group Failures 647
 - Detecting Physical Interface Repairs 648
 - What Happens During Interface Failover 648
 - IPMP and Dynamic Reconfiguration 649
 - Attaching NICs 650
 - Detaching NICs 651
 - Reattaching NICs 651
 - NICs That Were Missing at System Boot 651

- 30 Administering IPMP (Tasks) 653**
 - Configuring IPMP (Task Maps) 653
 - Configuring and Administering IPMP Groups (Task Map) 654
 - Administering IPMP on Interfaces That Support Dynamic Reconfiguration (Task Map) 655
 - Configuring IPMP Groups 655
 - Planning for an IPMP Group 655
 - ▼ How to Plan for an IPMP Group 655

▼ SPARC: How to Ensure That the MAC Address of an Interface Is Unique	657
Configuring IPMP Groups	659
▼ How to Configure an IPMP Group With Multiple Interfaces	659
Configuring IPMP Groups With a Single Physical Interface	667
▼ How to Configure a Single Interface IPMP Group	667
Maintaining IPMP Groups	668
▼ How to Display the IPMP Group Membership of an Interface	669
▼ How to Add an Interface to an IPMP Group	669
▼ How to Remove an Interface From an IPMP Group	670
▼ How to Move an Interface From One IPMP Group to Another Group	671
Replacing a Failed Physical Interface on Systems That Support Dynamic Reconfiguration	672
▼ How to Remove a Physical Interface That Has Failed (DR-Detach)	672
▼ How to Replace a Physical Interface That Has Failed (DR-Attach)	673
Recovering a Physical Interface That Was Not Present at System Boot	674
▼ How to Recover a Physical Interface That Was Not Present at System Boot	675
Modifying the <code>/etc/default/mpathd</code> IPMP Configuration File	677
▼ How to Configure the <code>/etc/default/mpathd</code> File	677

Part VII IP Quality of Service (IPQoS) 679

31 Introducing IPQoS (Overview)	681
IPQoS Basics	681
What Are Differentiated Services?	681
IPQoS Features	682
Where to Get More Information About Quality-of-Service Theory and Practice	682
Providing Quality of Service With IPQoS	684
Implementing Service-Level Agreements	684
Assuring Quality of Service for an Individual Organization	684
Introducing the Quality-of-Service Policy	684
Improving Network Efficiency With IPQoS	685
How Bandwidth Affects Network Traffic	685
Using Classes of Service to Prioritize Traffic	686
Differentiated Services Model	687
Classifier (<code>ipgpc</code>) Overview	687

	Meter (tokenmt and tswtclmt) Overview	688
	Marker (dscpmk and dlcosmk) Overview	689
	Flow Accounting (flowacct) Overview	689
	How Traffic Flows Through the IPQoS Modules	690
	Traffic Forwarding on an IPQoS-Enabled Network	691
	DS Codepoint	691
	Per-Hop Behaviors	692
32	Planning for an IPQoS-Enabled Network (Tasks)	695
	General IPQoS Configuration Planning (Task Map)	695
	Planning the Diffserv Network Topology	696
	Hardware Strategies for the Diffserv Network	696
	IPQoS Network Topologies	697
	Planning the Quality-of-Service Policy	699
	QoS Policy Planning Aids	699
	QoS Policy Planning (Task Map)	700
	▼ How to Prepare a Network for IPQoS	701
	▼ How to Define the Classes for Your QoS Policy	702
	Defining Filters	704
	▼ How to Define Filters in the QoS Policy	705
	▼ How to Plan Flow Control	706
	▼ How to Plan Forwarding Behavior	708
	▼ How to Plan for Flow Accounting	710
	Introducing the IPQoS Configuration Example	711
	IPQoS Topology	711
33	Creating the IPQoS Configuration File (Tasks)	715
	Defining a QoS Policy in the IPQoS Configuration File (Task Map)	715
	Tools for Creating a QoS Policy	717
	Basic IPQoS Configuration File	717
	Creating IPQoS Configuration Files for Web Servers	718
	▼ How to Create the IPQoS Configuration File and Define Traffic Classes	720
	▼ How to Define Filters in the IPQoS Configuration File	722
	▼ How to Define Traffic Forwarding in the IPQoS Configuration File	724
	▼ How to Enable Accounting for a Class in the IPQoS Configuration File	727
	▼ How to Create an IPQoS Configuration File for a Best-Effort Web Server	728
	Creating an IPQoS Configuration File for an Application Server	731

	▼ How to Configure the IPQoS Configuration File for an Application Server	733
	▼ How to Configure Forwarding for Application Traffic in the IPQoS Configuration File	735
	▼ How to Configure Flow Control in the IPQoS Configuration File	737
	Providing Differentiated Services on a Router	741
	▼ How to Configure a Router on an IPQoS-Enabled Network	741
34	Starting and Maintaining IPQoS (Tasks)	743
	Administering IPQoS (Task Map)	743
	Applying an IPQoS Configuration	744
	▼ How to Apply a New Configuration to the IPQoS Kernel Modules	744
	▼ How to Ensure That the IPQoS Configuration Is Applied After Each Reboot	745
	Enabling <code>syslog</code> Logging for IPQoS Messages	746
	▼ How to Enable Logging of IPQoS Messages During Booting	746
	Troubleshooting with IPQoS Error Messages	747
35	Using Flow Accounting and Statistics Gathering (Tasks)	751
	Setting Up Flow Accounting (Task Map)	751
	Recording Information About Traffic Flows	752
	▼ How to Create a File for Flow-Accounting Data	752
	Gathering Statistical Information	754
36	IPQoS in Detail (Reference)	757
	IPQoS Architecture and the Diffserv Model	757
	Classifier Module	758
	Meter Module	760
	Marker Module	763
	<code>flowacct</code> Module	767
	IPQoS Configuration File	770
	<code>action</code> Statement	771
	Module Definitions	772
	<code>class</code> Clause	772
	<code>filter</code> Clause	773
	<code>params</code> Clause	773
	<code>ipqosconf</code> Configuration Utility	774

Glossary 775

Index 787

Preface

System Administration Guide, IP Services is part of a nine-volume set that covers a significant part of the Solaris™ system administration information. This book assumes that you have already installed the Solaris 10 operating system (Solaris OS). You should be ready to configure your network or ready to configure any networking software that is required on your network. The Solaris OS 10 is part of the Solaris product family, which also includes the Solaris Common Desktop Environment (CDE). Solaris OS is compliant with AT&T's System V, Release 4 operating system.

Note – This Solaris release supports systems that use the SPARC® and x86 families of processor architectures: UltraSPARC®, SPARC64, AMD64, Pentium, and Xeon EM64T. The supported systems appear in the *Solaris 10 Hardware Compatibility List* at <http://www.sun.com/bigadmin/hcl>. This document cites any implementation differences between the platform types.

In this document the term “x86” refers to 64-bit and 32-bit systems manufactured using processors compatible with the AMD64 or Intel Xeon/Pentium product families. For supported systems, see the *Solaris 10 Hardware Compatibility List*.

Who Should Use This Book

This book is intended for anyone responsible for administering systems that run the Solaris OS release, which are configured in a network. To use this book, you should have at least two years of UNIX® system administration experience. Attending UNIX system administration training courses might be helpful.

How the System Administration Volumes Are Organized

Here is a list of the topics that are covered by the volumes of the System Administration Guides.

Book Title	Topics
<i>System Administration Guide: Basic Administration</i>	User accounts and groups, server and client support, shutting down and booting a system, managing services, and managing software (packages and patches)
<i>System Administration Guide: Advanced Administration</i>	Printing services, terminals and modems, system resources (disk quotas, accounting, and crontabs), system processes, and troubleshooting Solaris software problems
<i>System Administration Guide: Devices and File Systems</i>	Removable media, disks and devices, file systems, and backing up and restoring data
<i>System Administration Guide: IP Services</i>	TCP/IP network administration, IPv4 and IPv6 address administration, DHCP, IPsec, IKE, Solaris IP filter, Mobile IP, IP network multipathing (IPMP), and IPQoS
<i>System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)</i>	DNS, NIS, and LDAP naming and directory services, including transitioning from NIS to LDAP and transitioning from NIS+ to LDAP
<i>System Administration Guide: Naming and Directory Services (NIS+)</i>	NIS+ naming and directory services
<i>System Administration Guide: Network Services</i>	Web cache servers, time-related services, network file systems (NFS and Autofs), mail, SLP, and PPP
<i>System Administration Guide: Security Services</i>	Auditing, device management, file security, BART, Kerberos services, PAM, Solaris cryptographic framework, privileges, RBAC, SASL, and Solaris Secure Shell
<i>System Administration Guide: Solaris Containers—Resource Management and Solaris Zones</i>	Resource management topics projects and tasks, extended accounting, resource controls, fair share scheduler (FSS), physical memory control using the resource capping daemon (rcapd), and dynamic resource pools; virtualization using Solaris Zones software partitioning technology

Related Books

The following trade books are referred to in this book.

- Stevens, W. Richard. *TCP/IP Illustrated, Volume 1, The Protocols*. Addison Wesley, 1994.
- Hunt Craig. *TCP/IP Network Administration, 3rd Edition*. O'Reilly, 2002.
- Perkins, Charles E. *Mobile IP Design Principles and Practices*. Massachusetts, 1998, Addison-Wesley Publishing Company.
- Solomon, James D. *Mobile IP: The Internet Unplugged*. New Jersey, 1998, Prentice-Hall, Inc.
- Ferguson, Paul and Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Related Third-Party Web Site References

Third party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Solaris IP Filter is derived from open source IP Filter software. To view license terms, attribution, and copyright statements for IP Filter, the default path is `/usr/lib/ipf/IPFILTER.LICENCE`. If Solaris OS has been installed anywhere other than the default, modify the given path to access the file at the installed location.

Accessing Sun Documentation Online

The docs.sun.comSM Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is <http://docs.sun.com>.

Ordering Sun Documentation

Sun Microsystems offers select product documentation in print. For a list of documents and how to order them, see “Buy printed documentation” at <http://docs.sun.com>.

Typographic Conventions

The following table describes the typographic changes that are used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> you have mail.
AaBbCc123	What you type, contrasted with onscreen computer output	<code>machine_name%</code> su Password:
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	The command to remove a file is <code>rm filename</code> .

TABLE P-1 Typographic Conventions (Continued)

Typeface or Symbol	Meaning	Example
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . Perform a <i>patch analysis</i> . Do <i>not</i> save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	machine_name%
C shell superuser prompt	machine_name#
Bourne shell and Korn shell prompt	\$
Bourne shell and Korn shell superuser prompt	#

PART I

Introducing System Administration: IP Services

This part contains introductory information about the TCP/IP protocol suite and its implementation in the Solaris Operating System (Solaris OS).

Fundamentals of TCP/IP (Overview)

This chapter introduces the Solaris implementation of the TCP/IP network protocol suite. The information is intended for system and network administrators who are unfamiliar with basic TCP/IP concepts. The remaining parts of this book assume that you are familiar with these concepts.

This chapter contains the following information:

- “Introducing the Internet Protocol Suite” on page 35
- “How the TCP/IP Protocols Handle Data Communications” on page 43
- “Finding Out More About TCP/IP and the Internet” on page 47

Introducing the Internet Protocol Suite

This section presents an in-depth introduction to the protocols that are included in TCP/IP. Although the information is conceptual, you should learn the names of the protocols and what each protocol does.

“TCP/IP” is the acronym that is commonly used for the set of network protocols that compose the *Internet Protocol suite*. Many texts use the term “Internet” to describe both the protocol suite and the global wide area network. In this book, “TCP/IP” refers specifically to the Internet protocol suite. “Internet” refers to the wide area network and the bodies that govern the Internet.

To interconnect your TCP/IP network with other networks, you must obtain a unique IP address for your network. At the time of this writing, you obtain this address from an Internet service provider (ISP).

If hosts on your network are to participate in the Internet Domain Name System (DNS), you must obtain and register a unique domain name. The InterNIC coordinates the registration of domain names through a group of worldwide registries. For more information on DNS, refer to *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Protocol Layers and the Open Systems Interconnection Model

Most network protocol suites are structured as a series of layers, sometimes collectively referred to as a *protocol stack*. Each layer is designed for a specific purpose. Each layer exists on both the sending and receiving systems. A specific layer on one system sends or receives exactly the same object that another system's *peer process* sends or receives. These activities occur independently from activities in layers above or below the layer under consideration. In essence, each layer on a system acts independently of other layers on the same system. Each layer acts in parallel with the same layer on other systems.

OSI Reference Model

Most network protocol suites are structured in layers. The International Organization for Standardization (ISO) designed the Open Systems Interconnection (OSI) Reference Model that uses structured layers. The OSI model describes a structure with seven layers for network activities. One or more protocols is associated with each layer. The layers represent data transfer operations that are common to all types of data transfers among cooperating networks.

The OSI model lists the protocol layers from the top (layer 7) to the bottom (layer 1). The following table shows the model.

TABLE 1-1 Open Systems Interconnection Reference Model

Layer No.	Layer Name	Description
7	Application	Consists of standard communication services and applications that everyone can use.
6	Presentation	Ensures that information is delivered to the receiving system in a form that the system can understand.
5	Session	Manages the connections and terminations between cooperating systems.
4	Transport	Manages the transfer of data. Also assures that the received data are identical to the transmitted data.

TABLE 1-1 Open Systems Interconnection Reference Model (Continued)

Layer No.	Layer Name	Description
3	Network	Manages data addressing and delivery between networks.
2	Data link	Handles the transfer of data across the network media.
1	Physical	Defines the characteristics of the network hardware.

The OSI model defines conceptual operations that are not unique to any particular network protocol suite. For example, the OSI network protocol suite implements all seven layers of the OSI model. TCP/IP uses some of OSI model layers. TCP/IP also combines other layers. Other network protocols, such as SNA, add an eighth layer.

TCP/IP Protocol Architecture Model

The OSI model describes idealized network communications with a family of protocols. TCP/IP does not directly correspond to this model. TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all. The following table shows the layers of the Solaris implementation of TCP/IP. The table lists the layers from the topmost layer (application) to the bottommost layer (physical network).

TABLE 1-2 TCP/IP Protocol Stack

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	Application	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP, SCTP
3	Network	Internet	IPv4, IPv6, ARP, ICMP
2	Data link	Data link	PPP, IEEE 802.2
1	Physical	Physical network	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI, and others

The table shows the TCP/IP protocol layers and the OSI model equivalents. Also shown are examples of the protocols that are available at each level of the TCP/IP protocol stack. Each system that is involved in a communication transaction runs a unique implementation of the protocol stack.

Physical Network Layer

The *physical network layer* specifies the characteristics of the hardware to be used for the network. For example, physical network layer specifies the physical characteristics of the communications media. The physical layer of TCP/IP describes hardware standards such as IEEE 802.3, the specification for Ethernet network media, and RS-232, the specification for standard pin connectors.

Data-Link Layer

The *data-link layer* identifies the network protocol type of the packet, in this instance TCP/IP. The data-link layer also provides error control and “framing.” Examples of data-link layer protocols are Ethernet IEEE 802.2 framing and Point-to-Point Protocol (PPP) framing.

Internet Layer

The Internet layer, also known as the *network layer* or *IP layer*, accepts and delivers packets for the network. This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP).

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

- **IP addressing** – The IP addressing conventions are part of the IP protocol. “[Designing an IPv4 Addressing Scheme](#)” on page 57 introduces IPv4 addressing and “[IPv6 Addressing Overview](#)” on page 74 introduces IPv6 addressing.
- **Host-to-host communications** – IP determines the path a packet must take, based on the receiving system’s IP address.
- **Packet formatting** – IP assembles packets into units that are known as *datagrams*. Datagrams are fully described in “[Internet Layer: Where Packets Are Prepared for Delivery](#)” on page 45.
- **Fragmentation** – If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet.

The Solaris OS supports both IPv4 and IPv6 addressing formats, which are described in this book. To avoid confusion when addressing the Internet Protocol, one of the following conventions is used:

- When the term “IP” is used in a description, the description applies to both IPv4 and IPv6.

- When the term “IPv4” is used in a description, the description applies only to IPv4.
- When the term “IPv6” is used in a description, the description applies only to IPv6.

ARP Protocol

The Address Resolution Protocol (ARP) conceptually exists between the data-link and Internet layers. ARP assists IP in directing datagrams to the appropriate receiving system by mapping Ethernet addresses (48 bits long) to known IP addresses (32 bits long).

ICMP Protocol

The Internet Control Message Protocol (ICMP) detects and reports network error conditions. ICMP reports on the following:

- **Dropped packets** – Packets that arrive too fast to be processed
- **Connectivity failure** – A destination system cannot be reached
- **Redirection** – Redirecting a sending system to use another router

[Chapter 7](#) contains more information on the Solaris OS commands that use ICMP for error detection.

Transport Layer

The TCP/IP *transport layer* ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets. This type of communication is known as *end-to-end*. Transport layer protocols at this level are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). TCP and SCTP provide reliable, end-to-end service. UDP provides unreliable datagram service.

TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets. This transmission consists of the following:

- Starting point, which opens the connection
- Entire transmission in byte order
- Ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains many parameters that help processes on the sending system connect to peer processes on the receiving system.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a “reliable, connection-oriented” protocol.

SCTP Protocol

SCTP is a reliable, connection-oriented transport layer protocol that provides the same services to applications that are available from TCP. Moreover, SCTP can support connections between systems that have more than one address, or *multi-homed*. The SCTP connection between sending and receiving system is called an *association*. Data in the association is organized in chunks. Because SCTP supports multi-homing, certain applications, particularly applications used by the telecommunications industry, need to run over SCTP, rather than TCP.

UDP Protocol

UDP provides datagram delivery service. UDP does not verify connections between receiving and sending hosts. Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use UDP.

Application Layer

The *application layer* defines standard Internet services and network applications that anyone can use. These services work with the transport layer to send and receive data. Many application layer protocols exist. The following list shows examples of application layer protocols:

- Standard TCP/IP services such as the `ftp`, `tftp`, and `telnet` commands
- UNIX “r” commands, such as `rlogin` and `rsh`
- Name services, such as NIS and the domain name system (DNS)
- Directory services (LDAP)
- File services, such as the NFS service
- Simple Network Management Protocol (SNMP), which enables network management
- Router Discovery Server protocol (RDISC) and Routing Information Protocol (RIP) routing protocols

Standard TCP/IP Services

- **FTP and Anonymous FTP** – The File Transfer Protocol (FTP) transfers files to and from a remote network. The protocol includes the `ftp` command and the `in.ftpd` daemon. FTP enables a user to specify the name of the remote host and file transfer command options on the local host’s command line. The `in.ftpd` daemon on the

remote host then handles the requests from the local host. Unlike `rcp`, `ftp` works even when the remote computer does not run a UNIX based operating system. A user must log in to the remote system to make an `ftp` connection, unless the remote system has been configured to allow anonymous FTP.

You can obtain an enormous amount of material from *anonymous FTP servers* that are connected to the Internet. Universities and other institutions set up these servers to offer software, research papers, and other information to the public domain. When you log in to this type of server, you use the login name `anonymous`, hence the term “anonymous FTP server.”

Using anonymous FTP and setting up anonymous FTP servers is outside the scope of this manual. However, many books, such as *The Whole Internet User's Guide & Catalog*, discuss anonymous FTP in detail. Instructions for using FTP are in *System Administration Guide: Network Services*. The `ftp(1)` man page describes all `ftp` command options that are invoked through the command interpreter. The `ftpd(1M)` man page describes the services that are provided by the `in.ftpd` daemon.

- **Telnet** – The Telnet protocol enables terminals and terminal-oriented processes to communicate on a network that runs TCP/IP. This protocol is implemented as the `telnet` program on local systems and the `in.telnetd` daemon on remote machines. Telnet provides a user interface through which two hosts can communicate on a character-by-character or line-by-line basis. Telnet includes a set of commands that are fully documented in the `telnet(1)` man page.
- **TFTP** – The Trivial File Transfer Protocol (`tftp`) provides functions that are similar to `ftp`, but the protocol does not establish `ftp`'s interactive connection. As a result, users cannot list the contents of a directory or change directories. A user must know the full name of the file to be copied. The `telnet(1)` man page describes the `tftp` command set.

UNIX “r” Commands

The UNIX “r” commands enable users to issue commands on their local machines that run on the remote host. These commands include the following:

- `rcp`
- `rlogin`
- `rsh`

Instructions for using these commands are in the `rcp(1)`, `rlogin(1)`, and `rsh(1)` man pages.

Name Services

The Solaris OS provides the following name services:

- **DNS** – The domain name system (DNS) is the name service provided by the Internet for TCP/IP networks. DNS provides host names to the IP address service. DNS also serves as a database for mail administration. For a complete description

of this service, see *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*. See also the `resolver(3RESOLV)` man page.

- **/etc files** – The original host-based UNIX name system was developed for standalone UNIX machines and then adapted for network use. Many old UNIX operating systems and computers still use this system, but it is not well suited for large complex networks.
- **NIS** – Network Information Service (NIS) was developed independently of DNS and has a slightly different focus. Whereas DNS focuses on making communication simpler by using machine names instead of numerical IP addresses, NIS focuses on making network administration more manageable by providing centralized control over a variety of network information. NIS stores information about machine names and addresses, users, the network itself, and network services. NIS name space information is stored in NIS maps. For more information on NIS Architecture and NIS Administration, see *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Directory Service

The Solaris OS supports LDAP (Lightweight Directory Access Protocol) in conjunction with the Sun Open Net Environment (Sun ONE) Directory Server, as well as other LDAP directory servers. The distinction between a name service and a directory service is in the differing extent of functionality. A directory service provides the same functionality of a naming service, but provides additional functionalities as well. See *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

File Services

The NFS application layer protocol provides file services for the Solaris OS. You can find complete information about the NFS service in *System Administration Guide: Network Services*.

Network Administration

The Simple Network Management Protocol (SNMP) enables you to view the layout of your network and the status of key machines. SNMP also enables you to obtain complex network statistics from software that is based on a graphical user interface (GUI). Many companies offer network management packages that implement SNMP.

Routing Protocols

The Routing Information Protocol (RIP) and the Router Discovery Server Protocol (RDISC) are two routing protocols for TCP/IP networks. They are described in “[Routing Protocols in the Solaris OS](#)” on page 201.

How the TCP/IP Protocols Handle Data Communications

When a user issues a command that uses a TCP/IP application layer protocol, a series of events is initiated. The user's command or message passes through the TCP/IP protocol stack on the local system. Then, the command or message passes across the network media to the protocols on the remote system. The protocols at each layer on the sending host add information to the original data.

Protocols on each layer of the sending host also interact with their peers on the receiving host. [Figure 1-1](#) shows this interaction.

Data Encapsulation and the TCP/IP Protocol Stack

The packet is the basic unit of information that is transferred across a network. The basic packet consists of a header with the sending and receiving systems' addresses, and a body, or *payload*, with the data to be transferred. As the packet travels through the TCP/IP protocol stack, the protocols at each layer either add or remove fields from the basic header. When a protocol on the sending system adds data to the packet header, the process is called *data encapsulation*. Moreover, each layer has a different term for the altered packet, as shown in the following figure.

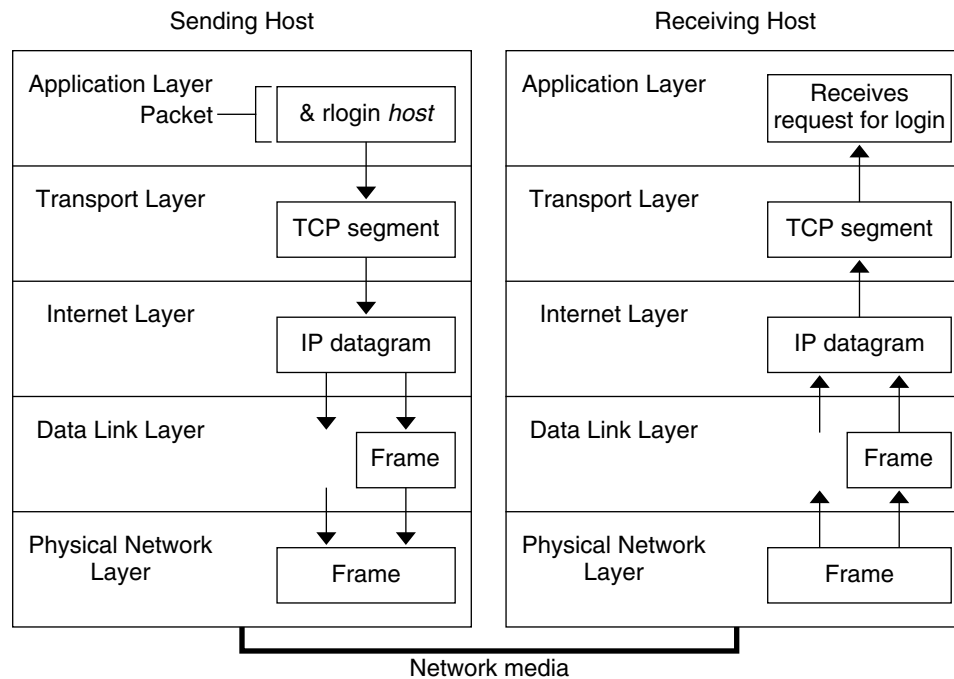


FIGURE 1-1 How a Packet Travels Through the TCP/IP Stack

This section summarizes the life cycle of a packet. The life cycle starts when you issue a command or send a message. The life cycle finishes when the appropriate application on the receiving system receives the packet.

Application Layer: Where a Communication Originates

The packet's history begins when a user on one system sends a message or issues a command that must access a remote system. The application protocol formats the packet so that the appropriate transport layer protocol, TCP or UDP, can handle the packet.

Suppose the user issues an `rlogin` command to log in to the remote system, as shown in Figure 1-1. The `rlogin` command uses the TCP transport layer protocol. TCP expects to receive data in the form of a stream of bytes that contain the information in the command. Therefore, `rlogin` sends this data as a TCP stream.

Transport Layer: Where Data Encapsulation Begins

When the data arrives at the transport layer, the protocols at the layer start the process of data encapsulation. The transport layer encapsulates the application data into transport protocol data units.

The transport layer protocol creates a virtual flow of data between the sending and receiving application, differentiated by the transport port number. The port number identifies a *port*, a dedicated location in memory for receiving or sending data. In addition, the transport protocol layer might provide other services, such as reliable, in order data delivery. The end result depends on whether TCP, SCTP, or UDP handles the information.

TCP Segmentation

TCP is often called a “connection-oriented” protocol because TCP ensures the successful delivery of data to the receiving host. [Figure 1-1](#) shows how the TCP protocol receives the stream from the `rlogin` command. TCP then divides the data that is received from the application layer into segments and attaches a header to each segment.

Segment headers contain sending and receiving ports, segment ordering information, and a data field that is known as a *checksum*. The TCP protocols on both hosts use the checksum data to determine if the data transfers without error.

Establishing a TCP Connection

TCP uses segments to determine whether the receiving system is ready to receive the data. When the sending TCP wants to establish connections, TCP sends a segment that is called a *SYN* to the TCP protocol on the receiving host. The receiving TCP returns a segment that is called an *ACK* to acknowledge the successful receipt of the segment. The sending TCP sends another *ACK* segment, then proceeds to send the data. This exchange of control information is referred to as a *three-way handshake*.

UDP Packets

UDP is a “connectionless” protocol. Unlike TCP, UDP does not check that data arrived at the receiving host. Instead, UDP formats the message that is received from the application layer into *UDP packets*. UDP attaches a header to each packet. The header contains the sending and receiving ports, a field with the length of the packet, and a checksum.

The sending UDP process attempts to send the packet to its peer UDP process on the receiving host. The application layer determines whether the receiving UDP process acknowledges the reception of the packet. UDP requires no notification of receipt. UDP does not use the three-way handshake.

Internet Layer: Where Packets Are Prepared for Delivery

The transport protocols TCP, UDP, and SCTP pass their segments and packets down to the Internet layer, where the IP protocol handles the segments and packets. IP prepares them for delivery by formatting them into units called *IP datagrams*. IP then determines the IP addresses for the datagrams, so that they can be delivered effectively to the receiving host.

IP Datagrams

IP attaches an *IP header* to the segment or packet's header, in addition to the information that is added by TCP or UDP. Information in the IP header includes the IP addresses of the sending and receiving hosts, the datagram length, and the datagram sequence order. This information is provided if the datagram exceeds the allowable byte size for network packets and must be fragmented.

Data-Link Layer: Where Framing Takes Place

Data-link layer protocols, such as PPP, format the IP datagram into a *frame*. These protocols attach a third header and a footer to "frame" the datagram. The frame header includes a *cyclic redundancy check* (CRC) field that checks for errors as the frame travels over the network media. Then, the data-link layer passes the frame to the physical layer.

Physical Network Layer: Where Frames Are Sent and Received

The physical network layer on the sending host receives the frames and converts the IP addresses into the hardware addresses appropriate to the network media. The physical network layer then sends the frame out over the network media.

How the Receiving Host Handles the Packet

When the packet arrives on the receiving host, the packet travels through the TCP/IP protocol stack in the reverse order from which it was sent. [Figure 1-1](#) illustrates this path. Moreover, each protocol on the receiving host strips off header information that is attached to the packet by its peer on the sending host. The following process occurs:

1. The physical network layer receives the packet in its frame form. The physical network layer computes the CRC of the packet, then sends the frame to the data link layer.
2. The data-link layer verifies that the CRC for the frame is correct and strips off the frame header and the CRC. Finally, the data-link protocol sends the frame to the Internet layer.
3. The Internet layer reads information in the header to identify the transmission. Then, the Internet layer determines if the packet is a fragment. If the transmission is fragmented, IP reassembles the fragments into the original datagram. IP then strips off the IP header and passes the datagram on to transport layer protocols.
4. The transport layer (TCP, SCTP, and UDP) reads the header to determine which application layer protocol must receive the data. Then, TCP, SCTP, or UDP strips off its related header. TCP, SCTP, or UDP sends the message or stream to the receiving application.

5. The application layer receives the message. The application layer then performs the operation that the sending host requested.

TCP/IP Internal Trace Support

TCP/IP provides internal trace support by logging TCP communication when an RST packet terminates a connection. When an RST packet is transmitted or received, information on as many as 10 packets, which were just transmitted, is logged with the connection information.

Finding Out More About TCP/IP and the Internet

Information about TCP/IP and the Internet is widely available. If you require specific information that is not covered in this text, you can probably find what you need in the sources cited next.

Computer Books About TCP/IP

Many trade books about TCP/IP and the Internet are available from your local library or computer bookstore. The following two books are considered the classic texts on TCP/IP:

- Craig Hunt. *TCP/IP Network Administration* – This book contains some theory and much practical information for managing a heterogeneous TCP/IP network.
- W. Richard Stevens. *TCP/IP Illustrated, Volume 1* – This book is an in-depth explanation of the TCP/IP protocols. This book is ideal for network administrators who require a technical background in TCP/IP and for network programmers.

TCP/IP and Networking Related Web Sites

The Internet has a wealth of web sites and user groups that are devoted to TCP/IP protocols and their administration. Many manufacturers, including Sun Microsystems, offer web-based resources for general TCP/IP information. The following are helpful web resources for TCP/IP information and general system administration information.

Web Site	Description
The Internet Engineering Task Force (IETF) web site (http://www.ietf.org/home.html)	The IETF is the body responsible for the architecture and governance of the Internet. The IETF web site contains information about the various activities of this organization. The site also includes links to the major publications of the IETF.
Sun Microsystem's BigAdmin Portal (http://www.sun.com/bigadmin)	BigAdmin provides information for administering Sun computers. The site offers FAQs, resources, discussions, links to documentation, and other materials that pertain to Solaris OS administration, including networking.

Requests for Comments and Internet Drafts

The Internet Engineering Task Force (IETF) working groups publish standards documents that are known as *Requests for Comments* (RFCs). Standards that are under development are published in *Internet Drafts*. The Internet Architecture Board (IAB) must approve all RFCs before they are placed in the public domain. Typically RFCs and Internet drafts are directed to developers and other highly technical readers. However, a number of RFCs that deal with TCP/IP topics contain valuable information for system administrators. These RFCs are cited in various places throughout this book.

Generally, For Your Information (FYI) documents appear as a subset of the RFCs. FYIs contain information that does not deal with Internet standards. FYIs contain Internet information of a more general nature. For example, FYI documents include a bibliography that list introductory TCP/IP books and papers. FYI documents provide an exhaustive compendium of Internet-related software tools. Finally, FYI documents include a glossary of Internet and general networking terms.

You will find references to relevant RFCs throughout this guide and other books in the Solaris System Administrator Collector.

PART II TCP/IP Administration

This part contains tasks and conceptual information for configuring, administering, and troubleshooting TCP/IP networks.

Planning Your TCP/IP Network (Tasks)

This chapter describes the issues you must resolve in order to create your network in an organized, cost-effective manner. After you resolve these issues, you can devise a network plan as you configure and administer your network in the future.

This chapter contains the following information:

- *“Determining the Network Hardware”* on page 53
- *“Obtaining Your Network’s IP Number”* on page 56
- *“Deciding on an IP Addressing Format for Your Network”* on page 54
- *“Naming Entities on Your Network”* on page 62
- *“Adding Routers to Your Network”* on page 64

For tasks for configuring a network, refer to [Chapter 5](#).

Network Planning (Task Map)

Task	Description	For Information
1. Plan your hardware requirements and network topology	Determine the types of equipment that you need and the layout of this equipment at your site.	<ul style="list-style-type: none"> ■ For general network topology questions, refer to “Determining the Network Hardware” on page 53. ■ For IPv6 topology planning, refer to “Preparing the Network Topology for IPv6 Support” on page 89. ■ For information about a specific type of equipment, refer to the equipment manufacturer’s documentation.
2. Obtain a registered IP address for your network	Your network must have a unique IP address if you plan to communicate outside your local network, for example, over the Internet.	Refer to “Obtaining Your Network’s IP Number” on page 56.
3. Devise an IP addressing scheme for your systems, based on your IPv4 network prefix or IPv6 site prefix.	Determine how addresses are to be deployed at your site.	Refer to “Designing an IPv4 Addressing Scheme” on page 57 or refer to “Preparing an IPv6 Addressing Plan” on page 92.
4. Create a list that contains the IP addresses and host names of all machines on your network.	Use the list to build network databases	Refer to “Network Databases” on page 63
5. Determine which name service to use on your network.	Decide whether to use NIS, LDAP, DNS, or the network databases in the local /etc directory.	Refer to “Selecting a Name Service and Directory Service” on page 62
6. Establish administrative subdivisions, if appropriate for your network	Decide if your site requires that you divide your network into administrative subdivisions	Refer to “Administrative Subdivisions” on page 64

Task	Description	For Information
7. Determine where to place routers in the your network design.	If your network is large enough to require routers, create a network topology that supports them.	Refer to “Adding Routers to Your Network” on page 64
8. If required, design a strategy for subnets.	You might need to create subnets for administering your IP address space or to make more IP addresses available for users.	For IPv4 subnet planning, refer to “What Is Subnetting?” on page 189 For IPv6 subnet planning, refer to

Determining the Network Hardware

When you design your network, you must decide what type of network best meets the needs of your organization. Some of the planning decisions you must make involve the following network hardware:

- The network topology, the layout, and connections of the network hardware
- The number of host systems your network can support
- The types of hosts that the network supports: standalone and dataless
- The types of servers that you might need
- The type of network media to use: Ethernet, Token Ring, FDDI, and so on
- Whether you need bridges or routers extend this media or connect the local network to external networks
- Whether some systems need separately purchased interfaces in addition to their built in interfaces

Based on these factors, you can determine the size of your local area network.

Note – How you plan the network hardware is outside the scope of this manual. For assistance, refer to the manuals that come with your hardware.

Deciding on an IP Addressing Format for Your Network

The number of systems that you expect to support affects how you configure your network. Your organization might require a small network of several dozen standalone systems that are located on one floor of a single building. Alternatively, you might need to set up a network with more than 1,000 systems in several buildings. This setup can require you to further divide your network into subdivisions that are called *subnets*.

When you plan your network addressing scheme, consider the following factors:

- The type of IP address that you want to use: IPv4 or IPv6
- The number of potential systems on your network
- The number of systems that are multihomed or routers, which require an IP address for each interface
- Whether to use private addresses on your network
- Whether to have a DHCP server that manages pools of IPv4 addresses

The worldwide growth of the Internet since 1990 has resulted in a shortage of available IP addresses. To remedy this situation, the Internet Engineering Task Force (IETF) has developed a number of IP addressing alternatives. Types of IP addresses in use today include the following:

If your organization has been assigned more than one IP address for your network or uses subnets, appoint a centralized authority within your organization to assign network IP addresses. That authority should maintain control of a pool of assigned network IP addresses, and assign network, subnet, and host addresses as required. To prevent problems, ensure that duplicate or random network numbers do not exist in your organization.

IPv4 Addresses

These 32-bit addresses are the original IP addressing format that was designed for TCP/IP. Originally, IP networks have three classes, A, B, and C. The *network number* that is assigned to a network reflects this class designation plus 8 or more bits to represent a host. Class-based IPv4 addresses require you to configure a netmask for the network number. Furthermore, to make more addresses available for systems on the local network, these addresses were often divided into subnets.

Today, IP addresses are referred to as *IPv4 addresses*. Although you can no longer obtain class-based IPv4 network numbers from an ISP, many existing networks still have them. For more information about administering IPv4 addresses, refer to “[Designing Your IPv4 Addressing Scheme](#)” on page 58.

IPv4 Addresses in CIDR Format

The IETF has developed Classless Inter-Domain Routing (CIDR) addresses as a short to medium term fix for the shortage of IPv4 addresses. In addition, CIDR format was designed as a remedy to the lack of capacity of the global Internet routing tables. An IPv4 address with CIDR notation is 32 bits in length and has the same dotted decimal format. However, CIDR adds a prefix designation after the rightmost byte to define the network portion of the IPv4 address. For more information, refer to [“Designing Your CIDR IPv4 Addressing Scheme”](#) on page 59.

DHCP Addresses

The Dynamic Host Configuration Protocol (DHCP) protocol enables a system to receive configuration information from a DHCP server, including an IP address, as part of the booting process. DHCP servers maintain pools of IP address from which to assign addresses to DHCP clients. A site that uses DHCP can use a smaller pool of IP addresses than would be needed if all clients were assigned a permanent IP address. You can set up the Solaris DHCP service to manage your site’s IP addresses, or a portion of the addresses. For more information, refer to [Chapter 11](#).

IPv6 Addresses

The IETF has deployed 128-bit IPv6 addresses as the long term solution to the shortage of available IPv4 addresses. IPv6 addresses provide greater address space than is available with IPv4. The Solaris OS supports IPv4 and IPv6 addressing on the same host, through the use of dual-stack TCP/IP. As with IPv4 addresses in CIDR format, IPv6 addresses have no notion of network classes or netmasks. As in CIDR, IPv6 addresses use prefixes to designate the portion of the address that defines the site’s network. For an introduction to IPv6, refer to [“IPv6 Addressing Overview”](#) on page 74.

Private Addresses and Documentation Prefixes

The IANA has reserved a block of IPv4 addresses and an IPv6 site prefix for use on private networks. You can deploy these addresses on systems within an enterprise network but be aware that packets with private addresses cannot be routed across the Internet. For more information on private addresses, refer to [“Using Private IPv4 Addresses”](#) on page 60.

Note – Private IPv4 addresses are also reserved for documentation purposes. The examples in this book use private IPv4 addresses and the reserved IPv6 documentation prefix.

Obtaining Your Network's IP Number

An IPv4 network is defined by a combination of an IPv4 network number plus a network mask, or *netmask*. An IPv6 network is defined by its *site prefix*, and, if subnetted, its *subnet prefix*.

Unless your network plans to be private in perpetuity, your local users most likely need to communicate beyond the local network. Therefore, you must obtain a registered IP number for your network from the appropriate organization before your network can communicate externally. This address becomes the network number for your IPv4 addressing scheme or the site prefix for your IPv6 addressing scheme.

Internet Service Providers (ISPs) provide IP addresses for networks with pricing that is based on different levels of service. Investigate with various ISPs to determine which provides the best service for your network. ISP's typically offer dynamically allocated addresses or static IP address to businesses. Some ISPs offer both IPv4 and IPv6 addresses.

If your site is an ISP, you obtain IP address blocks for your customers from the Internet Registry (IR) for your locale. The Internet Assigned Numbers Authority (IANA) is ultimately responsible for delegating registered IP addresses to IRs around the world. Each IR has registration information and templates for the locale that the IR services. For information about the IANA and its IRs, refer to the IANA's IP Address Service page (<http://www.iana.org/ipaddress/ip-addresses.htm>).

Note – Do not arbitrarily assign IP addresses to your network, even if you are not currently attaching the network to external TCP/IP networks. Instead, use private addresses as described in “Using Private IPv4 Addresses” on page 60.

Designing an IPv4 Addressing Scheme

Note – For IPv6 address planning information, refer to “[Preparing an IPv6 Addressing Plan](#)” on page 92.

This section gives an overview IPv4 addressing to aid you in designing an IPv4 addressing plan. For information on IPv6 addresses, see “[IPv6 Addressing Overview](#)” on page 74. For information on DHCP addresses, see [Chapter 11](#).

Each IPv4-based network must have the following:

- A unique network number that is assigned by either an ISP, an IR, or, for older networks, registered by the IANA. If you plan to use private addresses, the network numbers you devise must be unique within your organization.
- Unique IPv4 addresses for the interfaces of every system on the network.
- A network mask.

The IPv4 address is a 32-bit number that uniquely identifies a network interface on a system, as explained in “[How IP Addresses Apply to Network Interfaces](#)” on page 61. An IPv4 address is written in decimal digits, divided into four 8-bit fields that are separated by periods. Each 8-bit field represents a byte of the IPv4 address. This form of representing the bytes of an IPv4 address is often referred to as the *dotted-decimal format*.

The following figure shows the component parts of an IPv4 address, 172 . 16 . 50 . 56.

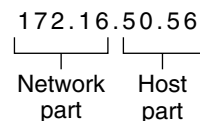


FIGURE 2-1 IPv4 Address Format

- | | |
|----------|--|
| 172 . 16 | Registered IPv4 network number. In class-based IPv4 notation, this number also defines the IP network class, Class B in this example, that would have been registered by the IANA. |
| 50 . 56 | Host part of the IPv4 address. The host part uniquely identifies an interface on a system on a network. Note that for each interface on a local network, the network part of the address is the same, but the host part must be different. |

If you plan to subnet a class-based IPv4 network, you need to define a subnet mask, or *netmask*, as explained in [“netmasks Database” on page 188](#).

The next example shows of the CIDR format address 192 . 168 . 3 . 56 / 22

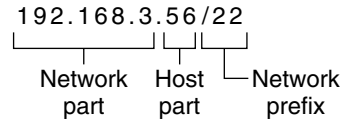


FIGURE 2-2 CIDR Format IPv4 Address

192 . 168 . 3	Network part, which consists of the IPv4 network number that is received from an ISP or IR.
56	Host part, which you assign to an interface on a system.
/22	Network prefix, which defines how many bits of the address comprise the network number. The network prefix also provides the subnet mask for the IP address. Network prefixes are also assigned by the ISP or IR.

A Solaris-based network can combine standard IPv4 addresses, CIDR format IPv4 addresses, DHCP addresses, IPv6 addresses, and private IPv4 addresses.

Designing Your IPv4 Addressing Scheme

This section describes the classes into which standard IPv4 address are organized. Though the IANA no longer gives out class-based network numbers, these network numbers are still in use on many networks. You might need to administer the address space for a site with class-based network numbers. For a complete discussion of IPv4 network classes, refer to [“Network Classes” on page 202](#).

The following table shows the division of the standard IPv4 address into network and host address spaces. For each class, “Range” specifies the range of decimal values for the first byte of the network number. “Network Address” indicates the number of bytes of the IPv4 address that are dedicated to the network part of the address. Each byte is represented by *xxx*. “Host Address” indicates the number of bytes that are dedicated to the host part of the address. For example, in a class A network address, the first byte is dedicated to the network, and the last three bytes are dedicated to the host. The opposite designation is true for a class C network.

TABLE 2-1 Division of the IPv4 Classes

Class	Byte Range	Network Number	Host Address
A	0–127	xxx	xxx.xxx.xxx
B	128–191	xxx.xxx	xxx.xxx
C	192–223	xxx.xxx.xxx	xxx

The numbers in the first byte of the IPv4 address define whether the network is class A, B, or C. The remaining three bytes have a range from 0–255. The two numbers 0 and 255 are reserved. You can assign the numbers 1–254 to each byte, depending on the network class that was assigned to your network by the IANA.

The following table shows which bytes of the IPv4 address are assigned to you. The table also shows the range of numbers within each byte that are available for you to assign to your hosts.

TABLE 2-2 Range of Available IPv4 Classes

Network Class	Byte 1 Range	Byte 2 Range	Byte 3 Range	Byte 4 Range
A	0–127	1–254	1–254	1–254
B	128–191	Preassigned by IANA	1–254	1–254
C	192–223	Preassigned by IANA	Preassigned by IANA	1–254

IPv4 Subnet Number

Local networks with large numbers of hosts are sometimes divided into subnets. If you divide your IPv4 network number into subnets, you need to assign a network identifier to each subnet. You can maximize the efficiency of the IPv4 address space by using some of the bits from the host part of the IPv4 address as a network identifier. When used as a network identifier, the specified part of the address becomes the subnet number. You create a subnet number by using a netmask, which is a bitmask that selects the network and subnet parts of an IPv4 address. Refer to [“Creating the Network Mask for IPv4 Addresses”](#) on page 189 for details.

Designing Your CIDR IPv4 Addressing Scheme

The network classes that originally constituted IPv4 are no longer in use on the global Internet. Today, the IANA distributes classless CIDR format addresses to its registries around the world. Any IPv4 address that you obtain from an ISP is in CIDR format, as shown in [Figure 2-2](#).

The network prefix of the CIDR address indicates how many IPv4 addresses are available for hosts on your network. Note that these host addresses are assigned to interfaces on a host. If a host has more than one physical interface, you need to assign a host address for every physical interface that is in use.

The network prefix of a CIDR address also defines the length of the subnet mask. Most Solaris 10 commands recognize the CIDR prefix designation of a network's subnet mask. However, the Solaris installation program and `/etc/netmask` file require you to set the subnet mask by using dotted decimal representation. In these two cases, use the dotted decimal representation of the CIDR network prefix, as shown in the next table.

TABLE 2-3 CIDR Prefixes and Their Decimal Equivalent

CIDR Network Prefix	Available IP Addresses	Dotted Decimal Subnet Equivalent
/19	8,192	255.255.224.0
/20	4,096	255.255.240.0
/21	2,048	255.255.248.0
/22	1024	255.255.252.0
/23	512	255.255.254.0
/24	256	255.255.255.0
/25	128	255.255.255.128
/26	64	255.255.255.192
/27	32	255.255.255.224

For more information on CIDR addresses, refer to the following sources:

- For technical details on CIDR, refer to RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy (<http://www.ietf.org/rfc/rfc1519.txt?number=1519>).
- More general information about CIDR is available from Pacific Bell Internet at Classless Inter-Domain Routing (CIDR) Overview (<http://public.pacbell.net/dedicated/cidr.html>).
- Another CIDR overview can be found in the Wikipedia article, "Classless inter-domain routing" (http://en.wikipedia.org/wiki/Classless_inter-domain_routing).

Using Private IPv4 Addresses

The IANA has reserved three blocks of IPv4 addresses for companies to use on their private networks. These addresses are defined in RFC 1918, Address Allocation for Private Internets (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>).

You can use these *private addresses*, also known as 1918 addresses, for systems on local networks within a corporate intranet. However, private addresses are not valid on the Internet. Do not use them on systems that must communicate outside the local network.

IPv4 Address Range	netmask
10.0.0.0 - 10.255.255.255	10.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0

How IP Addresses Apply to Network Interfaces

To connect to the network, a system must have at least one *physical network interface*. Each network interface must have its own unique IP address. During Solaris installation, you must supply the IP address for the first interface that the installation program finds. Usually that interface has the name *device-name0*, for example `eri0` or `hme0`. This interface is considered the *primary network interface*.

If you add a second network interface to a host, that interface also must have its own unique IP address. When you add the second network interface, the host then becomes *multihomed*. By contrast, when you add a second network interface to a host and enable IP forwarding, that host becomes a router. See [“Configuring a Router” on page 118](#) for an explanation.

Each network interface has a device name, a device driver, and an associated device file in the `/devices` directory. The network interface might have a device name such as `eri` or `smc0`, which are device names for two commonly used Ethernet interfaces.

For information and tasks related to interfaces, refer to [“Administering Physical Interfaces” on page 112](#).

Note – This book assumes that your systems have Ethernet network interfaces. If you plan to use different network media, refer to the manuals that come with the network interface for configuration information.

Naming Entities on Your Network

After you receive your assigned network IP address and you have given the IP addresses to your systems, the next task is to assign names to the hosts. Then you must determine how to handle name services on your network. You use these names initially when you set up your network and later when you expand your network through routers, bridges, or PPP.

The TCP/IP protocols locate a system on a network by using its IP address. However, if you use a recognizable name, then you can easily identify the system. Therefore, the TCP/IP protocols (and the Solaris OS) require both the IP address and the host name to uniquely identify a system.

From a TCP/IP perspective, a network is a set of named entities. A host is an entity with a name. A router is an entity with a name. The network is an entity with a name. A group or department in which the network is installed can also be given a name, as can a division, a region, or a company. In theory, the hierarchy of names that can be used to identify a network has virtually no limit. The domain name identifies a *domain*.

Administering Host Names

Many sites let users pick host names for their machines. Servers also require at least one host name, which is associated with the IP address of its primary network interface.

As a system administrator, you must ensure that each host name in your domain is unique. In other words, no two machines on your network can both have the name “fred.” However, the machine “fred” might have multiple IP addresses.

When planning your network, make a list of IP addresses and their associated host names for easy access during the setup process. The list can help you verify that all host names are unique.

Selecting a Name Service and Directory Service

The Solaris OS enables you to use three types of name services: local files, NIS, and DNS. Name services maintain critical information about the machines on a network, such as the host names, IP addresses, Ethernet addresses, and so forth. The Solaris OS also gives you the option of using the LDAP directory service in addition to or instead of a name service. For an introduction to name services on Solaris, refer to Part I, “About Naming and Directory Services,” in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Network Databases

When you install the operating system, you supply the host name and IP address of your server, clients, or standalone system as part of the procedure. The Solaris installation program adds this information into the `hosts` and `ipnodes` network databases. These databases are part of a set of network databases that contain information necessary for TCP/IP operation on your network. The name service that you select for your network reads these databases.

The configuration of the network databases is critical. Therefore, you need to decide which name service to use as part of the network planning process. Moreover, the decision to use name services also affects whether you organize your network into an administrative domain. “[Network Databases and the `nsswitch.conf` File](#)” on page 192 has detailed information on the set of network databases.

Using NIS or DNS as the Name Service

The NIS and DNS name services maintain network databases on several servers on the network. *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* describes these name services and explains how to configure the databases. In addition, the guide explain the “namespace” and “administrative domain” concepts in detail.

Using Local Files as the Name Service

If you do not implement NIS, LDAP, or DNS, the network uses *local files* to provide the name service. The term “local files” refers to the series of files in the `/etc` directory that the network databases use. The procedures in this book assume you are using local files for your name service, unless otherwise indicated.

Note – If you decide to use local files as the name service for your network, you can set up another name service at a later date.

Domain Names

Many networks organize their hosts and routers into a hierarchy of administrative domains. If you are using the NIS or DNS name service, you must select a domain name for your organization that is unique worldwide. To ensure that your domain name is unique, you should register the domain name with the InterNIC. If you plan to use DNS, you also need to register your domain name with the InterNIC.

The domain name structure is hierarchical. A new domain typically is located below an existing, related domain. For example, the domain name for a subsidiary company can be located below the domain of the parent company. If the domain name has no other relationship, an organization can place its domain name directly under one of the existing top-level domains.

The following are a few examples of top-level domains:

- .com – Commercial companies (international in scope)
- .edu – Educational institutions (international in scope)
- .gov – U.S. government agencies
- .fr – France

You select the name that identifies your organization, with the provision that the name must be unique.

Administrative Subdivisions

The question of administrative subdivisions deals with matters of size and control. The more hosts and servers that you have in a network, the more complex your management task. You might want to handle such situations by setting up additional administrative divisions. Add networks of a particular class. Divide existing networks into subnets. The decision about setting up administrative subdivisions for your network is determined by the following factors:

- **How large is the network?**

A single administrative division can handle a single network of several hundred hosts, all in the same physical location and requiring the same administrative services. However, sometimes you should establish several administrative subdivisions. Subdivisions are particularly useful if you have a small network with subnets and the network is scattered over an extensive geographical area.

- **Do users on the network have similar needs?**

For example, you might have a network that is confined to a single building and supports a relatively small number of machines. These machines are divided among a number of subnetworks. Each subnetwork supports groups of users with different needs. In this example, you might use an administrative subdivision for each subnet.

Adding Routers to Your Network

Recall that in TCP/IP, two types of entities exist on a network: hosts and routers. All networks must have hosts, while not all networks require routers. The physical topology of the network determines if you need routers. This section introduces the concepts of network topology and routing. These concepts are important when you decide to add another network to your existing network environment.

Network Topology Overview

Network topology describes how networks fit together. Routers are the entities that connect networks to each other. A router is any machine that has two or more network interfaces and implements IP forwarding. However, the system cannot function as a router until properly configured, as described in “Configuring a Router” on page 118.

Routers connect two or more networks to form larger internetworks. The routers must be configured to pass packets between two adjacent networks. The routers also should be able to pass packets to networks that lie beyond the adjacent networks.

The following figure shows the basic parts of a network topology. The first illustration shows a simple configuration of two networks that are connected by a single router. The second illustration shows a configuration of three networks, interconnected by two routers. In the first example, Router R joins Network 1 and Network 2 into a larger internetwork. In the second example, Router R1 connects Networks 1 and 2. Router R2 connects Networks 2 and 3. The connections form a network that includes Networks 1, 2, and 3.

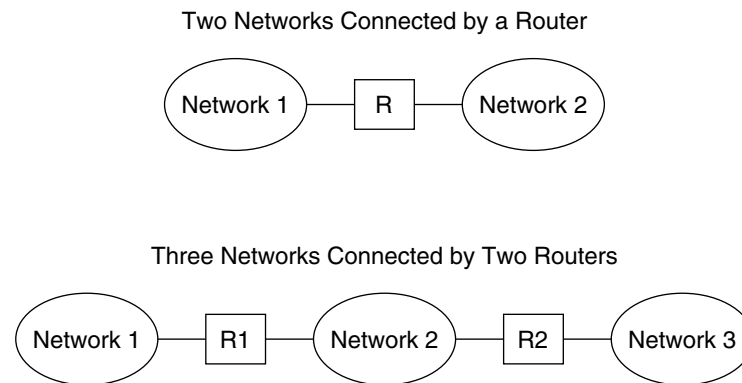


FIGURE 2-3 Basic Network Topology

In addition to joining networks into internetworks, routers route packets between networks that are based on the addresses of the destination network. As internetworks grow more complex, each router must make more and more decisions about the packet destinations.

The following figure shows a more complex case. Router R3 directly connects networks 1 and 3. The redundancy improves reliability. If network 2 goes down, router R3 still provides a route between networks 1 and 3. You can interconnect many networks. However, the networks must use the same network protocols.

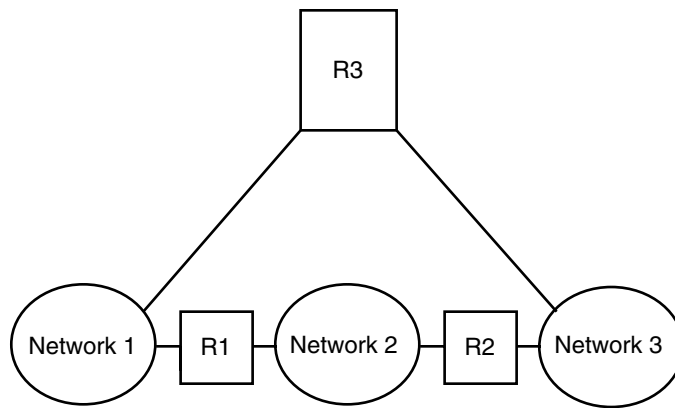


FIGURE 2-4 A Network Topology That Provides an Additional Path Between Networks

How Routers Transfer Packets

The IP address of the recipient, which is a part of the packet header, determines how the packet is routed. If this address includes the network number of the local network, the packet goes directly to the host with that IP address. If the network number is not the local network, the packet goes to the router on the local network.

Routers maintain routing information in *routing tables*. These tables contain the IP address of the hosts and routers on the networks to which the router is connected. The tables also contain pointers to these networks. When a router receives a packet, the router checks its routing table to determine if the table lists the destination address in the header. If the table does not contain the destination address, the router forwards the packet to another router that is listed in its routing table. Refer to [“Configuring a Router” on page 118](#) for detailed information on routers.

The following figure shows a network topology with three networks that are connected by two routers.

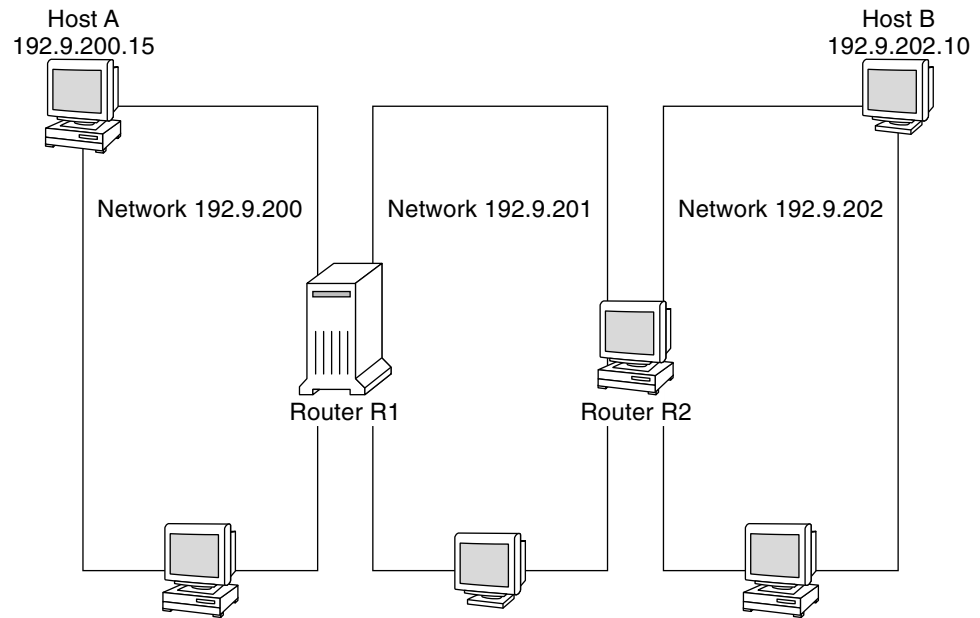


FIGURE 2-5 A Network Topology With Three Interconnected Networks

Router R1 connects networks 192 . 9 . 200 and 192 . 9 . 201. Router R2 connects networks 192 . 9 . 201 and 192 . 9 . 202. If Host A on network 192 . 9 . 200 sends a message to Host B on network 192 . 9 . 202, the following events occur:

1. Host A sends a packet out over network 192 . 9 . 200. The packet header contains the IPv4 address of the recipient Host B, 192 . 9 . 202 . 10.
2. None of the machines on network 192 . 9 . 200 has the IPv4 address 192 . 9 . 202 . 10. Therefore, Router R1 accepts the packet.
3. Router R1 examines its routing tables. No machine on network 192 . 9 . 201 has the address 192 . 9 . 202 . 10. However, the routing tables do list Router R2.
4. R1 then selects R2 as the “next hop” Router. R1 sends the packet to R2.
5. Because R2 connects network 192 . 9 . 201 to 192 . 9 . 202, R2 has routing information for Host B. Router R2 then forwards the packet to network 192 . 9 . 202, where Host B accepts the packet.

Introducing IPv6 (Overview)

This chapter presents an overview of the Solaris Internet Protocol version 6 (IPv6) implementation. This implementation includes the associated daemon and utilities that support the IPv6 address space.

IPv6 and IPv4 addresses coexist in the Solaris networking environment. Systems that are configured with IPv6 addresses retain their IPv4 addresses, if these addresses already exist. Operations that involve IPv6 addresses do not adversely affect IPv4 operations, and vice versa.

The following major topics are discussed:

- “Major Features of IPv6” on page 69
- “IPv6 Network Overview” on page 72
- “IPv6 Addressing Overview” on page 74
- “IPv6 Neighbor Discovery Protocol Overview” on page 81
- “IPv6 Address Autoconfiguration” on page 82
- “Overview of IPv6 Tunnels” on page 83

For more detailed information about IPv6, consult the following chapters.

- IPv6 network planning – [Chapter 4](#)
- IPv6-related tasks – [Chapter 6](#), [Chapter 7](#), and [Chapter 8](#)
- IPv6 details – [Chapter 10](#)

Major Features of IPv6

The defining feature of IPv6 is increased address space in comparison to IPv4. IPv6 also improves Internet capabilities in numerous areas, as outlined in this section.

Expanded Addressing

IP address size increases from 32 bits in IPv4 to 128 bits in IPv6, to support more levels of addressing hierarchy. In addition, IPv6 provides many more addressable IPv6 systems. For more information, see [“IPv6 Addressing Overview”](#) on page 74.

Address Autoconfiguration and Neighbor Discovery

The IPv6 *Neighbor Discovery (ND)* protocol facilitates the autoconfiguration of IPv6 addresses. *Autoconfiguration* is the ability of an IPv6 host to automatically generate its own IPv6 address, which makes address administration easier and less time-consuming. For more information, see [“IPv6 Address Autoconfiguration”](#) on page 82.

The Neighbor Discovery protocol corresponds to a combination of these IPv4 protocols: Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Router Discovery (RDISC), and ICMP Redirect. IPv6 routers use Neighbor Discovery to advertise the IPv6 site prefix. IPv6 hosts use Neighbor Discovery for various purposes, which include soliciting the prefix from an IPv6 router. For more information, see [“IPv6 Neighbor Discovery Protocol Overview”](#) on page 81.

Header Format Simplification

The IPv6 header format either drops or makes optional certain IPv4 header fields. This change keeps the bandwidth cost of the IPv6 header as low as possible, despite the increased address size. Even though IPv6 addresses are four times longer than IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.

Improved Support for IP Header Options

Changes in the way IP header options are encoded allow for more efficient forwarding. Also, IPv6 options have less stringent limits on their length. The changes provide greater flexibility for introducing new options in the future.

Application Support for IPv6 Addressing

Many critical Solaris network services recognize and support IPv6 addresses, for example:

- Name services, such as DNS, LDAP, and NIS. For more information on IPv6 support by these name services, see *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

- Authentication and privacy applications, such as IP Security Architecture (IPsec) and Internet Key Exchange (IKE). For more information, see [Part IV](#).
- Differentiated services, as provided by IP Quality of Service (IPQoS). For more information, see [Part VII](#).
- Failover detection, as provided by IP network multipathing (IPMP). For more information, see [Part VI](#).

Additional IPv6 Resources

In addition to this Part, you can obtain information about IPv6 from the sources that are listed in the following sections.

Requests for Comments and Internet Drafts

Many RFCs are available regarding IPv6. The following table lists the major IPv6 articles and their Internet Engineering Task Force (IETF) web locations as of this writing.

TABLE 3-1 IPv6-Related RFCs and Internet Drafts

RFC or Internet Draft	Subject	Location
RFC 2461, <i>Neighbor Discovery for IPv6 Version 6 (IPv6)</i>	Describes the features and functions of IPv6 Neighbor Discovery protocol	http://www.ietf.org/rfc/rfc2461.txt (http://www.ietf.org/rfc/rfc2461.txt?number=2461)
RFC 3306, <i>Unicast—Prefix—Based IPv6 Multicast Addresses</i>	Describes the format and types of IPv6 multicast addresses	ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt (ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt)
RFC 3484: <i>Default Address Selection for Internet Protocol version 6 (IPv6)</i>	Describes the algorithms used in IPv6 default address selection	http://www.ietf.org/rfc/rfc3484?number=3484 (http://www.ietf.org/rfc/rfc3484.txt?number=3484)
RFC 3513, <i>Internet Protocol version 6 (IPv6) Addressing Architecture</i>	Contains complete details about the types of IPv6 addresses and includes many examples	http://www.ietf.org/rfc/rfc3513.txt?number=3513 (http://www.ietf.org/rfc/rfc3513.txt?number=3513)
RFC 3587, <i>IPv6 Global Unicast Address Format</i>	Defines the standard format for IPv6 unicast addresses	http://www.ietf.org/rfc/rfc3587.txt?number=3587 (http://www.ietf.org/rfc/rfc3587.txt?number=3587)

Web Sites

The following web sites provide useful information about IPv6.

TABLE 3-2 IPv6-Related Web Sites

Web Site	Description	Location
IPv6 Forum	Links to IPv6-related presentations, events, classes, and implementations worldwide are available from this society's web site	http://www.ipv6forum.com
Internet Educational Task Force IPv6 Working Group	Links to all relevant IPv6 RFCs and Internet Drafts are on the home page of this IETF working group	http://www.ietf.org/html.charters/ipv6-charter.html
UK IPv6 Resource Center	Materials and links that are related to the <i>6bone</i> , the international test IPv6 network, and University of Lancaster IPv6 projects are on this web site of University of Lancaster UK	http://www.cs-ipv6.lancs.ac.uk

IPv6 Network Overview

This section introduces terms that are fundamental to the IPv6 network topology. The following figure shows the basic parts of an IPv6 network.

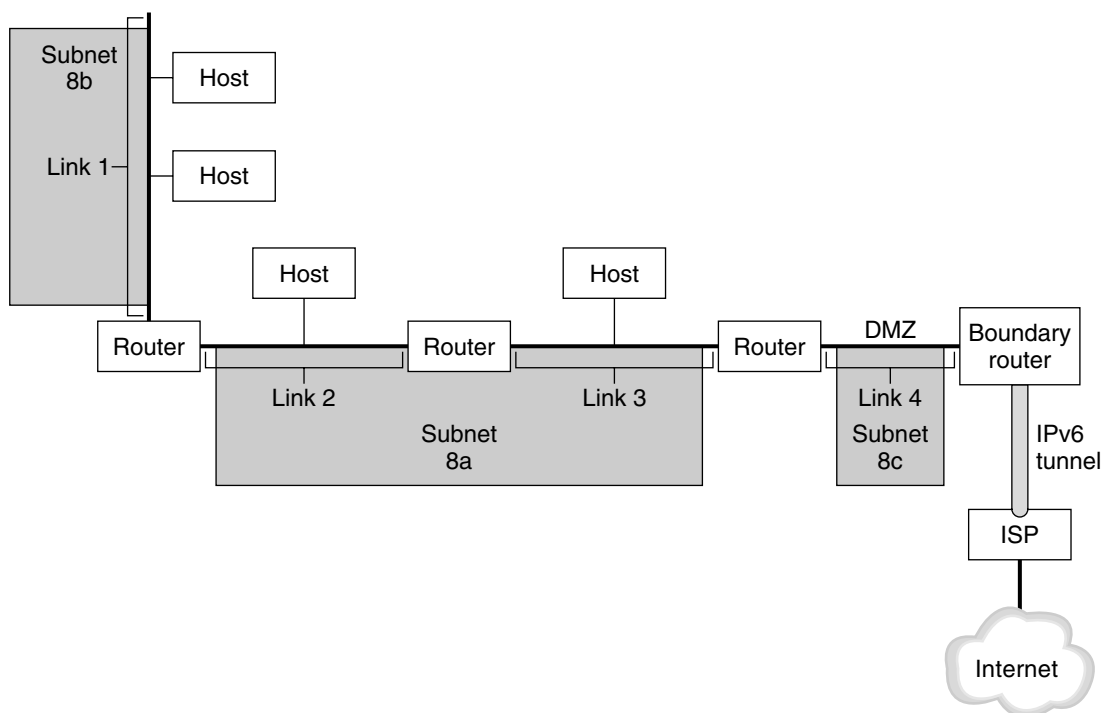


FIGURE 3-1 Basic Components of an IPv6 Network

The figure depicts an IPv6 network and its connection to an ISP. The internal network consists of Links 1, 2, 3, and 4. Each link is populated by hosts and terminated by a router. Link 4, which is the network's DMZ, is terminated on one end by the boundary router. The boundary router runs an IPv6 tunnel to an ISP, which provides Internet connectivity for the network. Links 2 and 3 are administered as Subnet 8a. Subnet 8b consists only of systems on Link 1. Subnet 8c is contiguous with the DMZ on Link 4.

As illustrated in [Figure 3-1](#), an IPv6 network has essentially the same components as an IPv4 network. However, IPv6 terminology differs slightly from IPv4 terminology. Here is a list of familiar terms for network components as they are used in an IPv6 context.

- node** Any system with an IPv6 address and interface that is configured for IPv6 support. This generic term applies to both hosts and routers.
- IPv6 router** A node that forwards IPv6 packets. At least one of the router's interfaces must be configured for IPv6 support. An IPv6 router can also advertise the registered IPv6 site prefix for the enterprise over the internal network.

IPv6 host	A node with an IPv6 address. An IPv6 host can have more than one interface that is configured for IPv6 support. As in IPv4, IPv6 hosts do not forward packets.
link	A single, contiguous network medium that is bounded on either end by a router.
neighbor	An IPv6 node that is on the same link as the local node.
IPv6 subnet	The administrative segment of an IPv6 network. Components of an IPv6 subnet can directly correspond to all nodes on a link, as in IPv4. Nodes on a link can be administered in separate subnets, if required. Additionally, IPv6 does support multilink subnets, where nodes on more than one link can be components of a single subnet. Links 2 and 3 in Figure 3-1 are components of multilink Subnet 8a.
IPv6 tunnel	A tunnel that provides a virtual point-to-point path between an IPv6 node and another IPv6 node endpoint. IPv6 supports manually configurable tunnels and automatic 6to4 tunnels.
boundary router	The router at the edge of a network that provides one end of the IPv6 tunnel to an endpoint outside the local network. This router must have at least one IPv6 interface to the internal network. For the external network, the router can have an IPv6 interface or an IPv4 interface.

IPv6 Addressing Overview

IPv6 addresses are assigned to interfaces, rather than to nodes, in recognition that a node can have more than one interface. Moreover, you can assign more than one IPv6 address to an interface.

Note – For complete technical information about the IPv6 address format, go to RFC 2374, IPv6 Global Unicast Address Format (<http://www.ietf.org/rfc/rfc2374.txt?number=2374>)

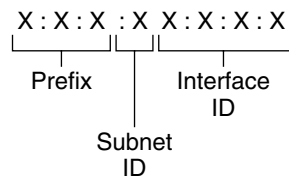
IPv6 defines three address types:

unicast	Identifies an interface of an individual node.
multicast	Identifies a group of interfaces, usually on different nodes. Packets that are sent to the multicast address go to all members of the <i>multicast group</i> .

anycast Identifies a group of interfaces, usually on different nodes. Packets that are sent to the anycast address go to the *anycast group* member node that is physically closest to the sender.

Parts of the IPv6 Address

An IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses. In the next figure, the x's represent hexadecimal numbers.



Example:

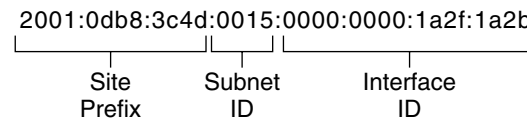


FIGURE 3-2 Basic IPv6 Address Format

The leftmost three fields (48 bits) contain the *site prefix*. The prefix describes the *public topology* that is usually allocated to your site by an ISP or Regional Internet Registry (RIR).

The next field is the 16-bit *subnet ID*, which you (or another administrator) allocate for your site. The subnet ID describes the *private topology*, also known as the *site topology*, because it is internal to your site.

The rightmost four fields (64 bits) contain the *interface ID*. The interface ID is either automatically configured from the interface's MAC address or manually configured in EUI-64 format.

Consider again the address in [Figure 3-2](#):

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

This example shows all 128 bits of an IPv6 address. The first 48 bits, `2001:0db8:3c4d`, contain the site prefix, representing the public topology. The next 16 bits, `0015`, contain the subnet ID, representing the private topology for the site. The lower order, rightmost 64 bits, `0000:0000:1a2f:1a2b`, contain the interface ID.

Abbreviating IPv6 Addresses

Most IPv6 addresses do not occupy all of their possible 128 bits. This condition results in fields that are padded with zeros or contain only zeros.

The IPv6 addressing architecture allows you use the two-colon (`::`) notation to represent contiguous 16-bit fields of zeros. For example, you might abbreviate the IPv6 address in [Figure 3–2](#) by replacing the two contiguous fields of zeros in the interface ID with two colons. The resulting address is `2001:0db8:3c4d:0015::1a2f:1a2b`. Other fields of zeros can be represented as a single 0. You can also omit any leading zeros in a field, such as changing `0db8` to `db8`.

So the address `2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b` can be abbreviated as `2001:db8:3c4d:15::1a2f:1a2b`.

You can use the two colon notation to replace any contiguous fields of all zeros in the IPv6 address. For example, the IPv6 address

`2001:0db8:3c4d:0015:0000:d234::3eee:0000` can be collapsed into `2001:db8:3c4d:15:0:d234:3eee::`.

Prefixes in IPv6

The leftmost fields of the IPv6 address contain the prefix, which is used for routing IPv6 packets. IPv6 prefixes have the following format:

prefix/length in bits

Prefix length is stated in classless inter-domain routing (CIDR) notation. CIDR notation is a slash at the end of the address that is followed by the prefix length in bits. For information on CIDR format IP addresses, refer to [“Designing Your CIDR IPv4 Addressing Scheme” on page 59](#).

The *site prefix* of an IPv6 address occupies up to 48 of the leftmost bits of the IPv6 address. For example, the site prefix of the IPv6 address `2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48` is contained in the leftmost 48 bits, `2001:db8:3c4d`. You use the following representation, with zeros compressed, to represent this prefix:

`2001:db8:3c4d::/48`

Note – The prefix `2001:db8::/32` is a special IPv6 prefix that is used specifically for documentation examples.

You can also specify a *subnet prefix*, which defines the internal topology of the network to a router. The example IPv6 address has the following subnet prefix.

`2001:db8:3c4d:15::/64`

The subnet prefix always contains 64 bits. These bits include 48 bits for the site prefix, in addition to 16 bits for the subnet ID.

The following prefixes have been reserved for special use:

`2002::/16` Indicates that a 6to4 routing prefix follows.
`fe80::/10` Indicates that a link-local address follows.
`ff00::/8` Indicates that a multicast address follows.

Unicast Addresses

IPv6 includes two different unicast address assignments:

- Global unicast address
- Link-local address

The type of unicast address is determined by the leftmost (high order) contiguous bits in the address, which contain the prefix.

The unicast address format is organized in the following hierarchy:

- Public topology
- Site (private) topology
- Interface ID

Global Unicast Address

The global unicast address is globally unique in the Internet. The example IPv6 address that is shown in “[Prefixes in IPv6](#)” on page 76 is a global unicast address. The next figure shows the scope of the global unicast address, as compared to the parts of the IPv6 address.

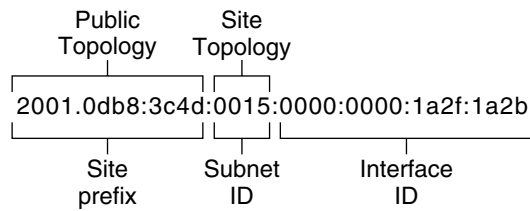


FIGURE 3-3 Parts of the Global Unicast Address

Public Topology

The site prefix defines the *public topology* of your network to a router. You obtain the site prefix for your enterprise from an ISP or Regional Internet Registry (RIR).

Site Topology and IPv6 Subnets

IN IPv6, the *subnet ID* defines an administrative subnet of the network and is up to 16 bits in length. You assign a subnet ID as part of IPv6 network configuration. The *subnet prefix* defines the site topology to a router by specifying the specific link to which the subnet has been assigned.

IPv6 subnets are conceptually the same as IPv4 subnets, in that each subnet is usually associated with a single hardware link. However, IPv6 subnet IDs are expressed in hexadecimal notation, rather than in dotted decimal notation.

Interface ID

The *interface ID* identifies an interface of a particular node. An interface ID must be unique within the subnet. IPv6 hosts can use the Neighbor Discovery protocol to automatically generate their own interface IDs. Neighbor Discovery automatically generates the interface ID, based on the MAC or EUI-64 address of the host's interface. You can also manually assign interface IDs, which is recommended for IPv6 routers and IPv6-enabled servers. For instructions on how to create a manual EUI-64 address, refer to RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture.

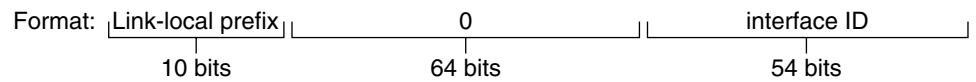
Transitional Global Unicast Addresses

For transition purposes, the IPv6 protocol includes the ability to embed an IPv4 address within an IPv6 address. This type of IPv4 address facilitates the tunneling of IPv6 packets over existing IPv4 networks. One example of a transitional global unicast address is the 6to4 address. For more information on 6to4 addressing, refer to “6to4 Automatic Tunnels” on page 237.

Link-Local Unicast Address

The link-local unicast address can be used only on the local network link. Link-local addresses are not valid nor recognized outside the enterprise. The following example shows the format of the link-local address.

EXAMPLE 3-1 Parts of the Link-Local Unicast Address



Example: fe80::123e:456d

A *link-local prefix* has the following format:

fe80::*interface-ID*/10

The following is an example of a link-local address:

fe80::23a1:b152

fe80 Hexadecimal representation of the 10-bit binary prefix 1111111010. This prefix identifies the type of IPv6 address as link local.

interface-ID Hexadecimal address of the interface, which is usually derived from the 48-bit MAC address.

When you enable IPv6 during Solaris installation, the lowest numbered interface on the local machine is configured with a link-local address. Each interface requires at least one link-local address to identify the node to other nodes on the local link. Therefore, you need to manually configure link-local addresses for additional interfaces of a node. After configuration, the node uses its link-local addresses for automatic address configuration and neighbor discovery.

Multicast Addresses

IPv6 supports the use of multicast addresses. The multicast address identifies a *multicast group*, which is a group of interfaces, usually on different nodes. An interface can belong to any number of multicast groups. If the first 16 bits of an IPv6 address is `ff00n`, the address is a multicast address.

Multicast addresses are used for sending information or services to all interfaces that are defined as members of the multicast group. For example, one use of multicast addresses is to communicate with all IPv6 nodes on the local link.

When an interface's IPv6 unicast address is created, the kernel automatically makes the interface a member of certain multicast groups. For example, the kernel makes each node a member of the Solicited Node multicast group, which is used by the Neighbor Discovery protocol to detect reachability. The kernel also automatically makes a node a member of the All-Nodes or All Routers multicast groups.

For detailed information about multicast addresses, refer to [“IPv6 Multicast Addresses in Depth” on page 207](#). For technical information, see RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses (<ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt>), which explains the multicast address format. For more information about the proper use of multicast addresses and groups, RFC 3307, Allocation Guidelines for IPv6 Multicast Addresses (<ftp://ftp.rfc-editor.org/in-notes/rfc3307.txt>).

Anycast Addresses and Groups

IPv6 anycast addresses identify a group of interfaces on different IPv6 nodes. Each group of interfaces is known as an *anycast group*. When a packet is sent to the anycast address, the anycast group member that is physically closest to the sender receives the packet.

Note – The Solaris Operating System (Solaris OS) implementation of IPv6 does not support the creation of anycast addresses and groups. However, Solaris IPv6 nodes can send packets to anycast addresses. For more information, see [“Considerations for Tunnels to a 6to4 Relay Router” on page 239](#).

IPv6 Neighbor Discovery Protocol Overview

IPv6 introduces the Neighbor Discovery protocol, which uses messaging as the means to handle the interaction between neighbor nodes. *Neighbor nodes* are IPv6 nodes that are on the same link. For example, by issuing neighbor discovery-related messages, a node can learn a neighbor's link-local address. Neighbor Discovery controls the following major activities on the IPv6 local link:

- **Router discovery** – Aids hosts in locating routers on the local link.
- **Address autoconfiguration** – Enables a node to automatically configure IPv6 addresses for its interfaces.
- **Prefix discovery** – Enables nodes to discover the known subnet prefixes that have been allocated to a link. Nodes use prefixes to distinguish destinations that are on the local link from those destinations that are only reachable through a router.
- **Address resolution** – Helps nodes to determine the link-local address of a neighbor, given only the destination's IP address.
- **Next-hop determination** – Uses an algorithm to determine the IP address of a packet recipient one hop that is beyond the local link. The next-hop can be a router or the destination node.
- **Neighbor unreachability detection** – Aids nodes to determine if a neighbor is no longer reachable. For both routers and hosts, address resolution can be repeated.
- **Duplicate address detection** – Enables a node to determine if an address that the node wants to use is not already in use.
- **Redirection** – Enables a router to inform a host of a better first-hop node to use to reach a particular destination.

Neighbor Discovery uses the following ICMP message types for communication among nodes on a link:

- Router solicitation
- Router advertisement
- Neighbor solicitation
- Neighbor advertisement
- Redirection

For detailed information on Neighbor Discovery messages and other Neighbor Discovery protocol topics, refer to “IPv6 Neighbor Discovery Protocol” on page 226. For technical information on Neighbor Discovery, see RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (<http://www.ietf.org/rfc/rfc2461.txt?number=2461>).

IPv6 Address Autoconfiguration

A major feature of IPv6 is a host's ability to autoconfigure an interface. Through Neighbor Discovery, the host locates an IPv6 router on the local link and requests a site prefix. The host does the following, as part of the autoconfiguration process:

- Creates a link-local address for each interface, which does not require a router on the link.
- Verifies the address's uniqueness on a link, which does not require a router on the link.
- Determines if the global addresses should be obtained through the stateless mechanism, the stateful mechanism, or both mechanisms. (Requires a router on the link.)

Note – Stateful autoconfiguration is achieved through DHCPv6. DHCPv6 is not supported in the current Solaris release.

Stateless Autoconfiguration Overview

Stateless autoconfiguration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism enables a host to generate its own addresses. The stateless mechanism uses local information as well as nonlocal information that is advertised by routers to generate the addresses.

You can implement temporary addresses for an interface, which are also autoconfigured. You enable a temporary address token for one or more interfaces on a host. However, unlike standard, autoconfigured IPv6 addresses, a temporary address consists of the site prefix and a randomly generated 64 bit number. This random number becomes the interface ID portion of the IPv6 address. A link-local address is not generated with the temporary address as the interface ID.

Routers advertise all prefixes that have been assigned on the link. IPv6 hosts use Neighbor Discovery to obtain a subnet prefix from a local router. Hosts automatically create IPv6 addresses by combining the subnet prefix with an interface ID that is generated from an interface's MAC address. In the absence of routers, a host can generate only link-local addresses. Link-local addresses can only be used for communication with nodes on the same link.

Note – Do not use stateless autoconfiguration to create the IPv6 addresses of servers. Hosts automatically generate interface IDs that are based on hardware-specific information during autoconfiguration. The current interface ID could become invalid if the existing interface is swapped for a new interface.

Overview of IPv6 Tunnels

For most enterprises, the introduction of IPv6 to an existing IPv4 network must occur on a gradual, step-by-step basis. The Solaris dual-stack network environment supports both IPv4 and IPv6 functionality. Because most networks use the IPv4 protocol, IPv6 networks currently require a way to communicate outside their borders. IPv6 networks use tunnels for this purpose.

In most IPv6 tunneling scenarios, the outbound IPv6 packet is encapsulated inside an IPv4 packet. The boundary router of the IPv6 network sets up a point-to-point tunnel over various IPv4 networks to the boundary router of the destination IPv6 network. The packet travels over the tunnel to the destination network's boundary router, which decapsulates the packet. Then, the router forwards the separate IPv6 packet to the destination node.

The Solaris IPv6 implementation supports the following tunneling scenarios:

- A manually configured tunnel between two IPv6 networks, over an IPv4 network. The IPv4 network can be the Internet or a local network within an enterprise.
- A manually configured tunnel between two IPv4 networks, over an IPv6 network, usually within an enterprise.
- A dynamically configured automatic 6to4 tunnel between two IPv6 networks, over an IPv4 network at an enterprise or over the Internet.

For detailed information about IPv6 tunnels, refer to [“IPv6 Tunnels” on page 233](#). For information about IPv- to-IPv4 tunnels and VPN, refer to [“Virtual Private Networks and IPsec” on page 436](#).

Planning an IPv6 Network (Tasks)

Deploying IPv6 on a new network or an existing network requires a major planning effort. This chapter contains the planning tasks that are necessary before you can configure IPv6 at your site. For existing networks, IPv6 deployment should be phased in gradually. The topics in this chapter help you phase in IPv6 onto an otherwise IPv4-only network.

The following topics are discussed in this chapter:

- “IPv6 Planning (Task Maps)” on page 85
- “IPv6 Network Topology Scenario” on page 87
- “Preparing the Existing Network to Support IPv6” on page 88
- “Preparing an IPv6 Addressing Plan” on page 92

For an introduction to IPv6 concepts, refer to [Chapter 3](#). For detailed information, refer to [Chapter 10](#).

IPv6 Planning (Task Maps)

Complete the tasks in the next task map in sequential order to accomplish the planning tasks necessary for IPv6 deployment.

Task	Description	For Instructions
1. Prepare your hardware to support IPv6.	Ensure that your hardware can be upgraded to IPv6.	“Preparing the Network Topology for IPv6 Support” on page 89

Task	Description	For Instructions
2. Get an ISP that supports IPv6.	Ensure that your current ISP supports IPv6. Otherwise, find an ISP who can support IPv6. You can use two ISPs, one ISP for IPv6 and one for ISP IPv4 communications.	
3. Ensure that your applications are IPv6 ready.	Verify that your applications can run in an IPv6 environment.	"How to Prepare Network Services for IPv6 Support" on page 90
4. Get a site prefix.	Obtain a 48-bit site prefix for your site from your ISP or from the nearest RIR.	"Obtaining a Site Prefix" on page 93
5. Create a subnet addressing plan.	You need to plan the overall IPv6 network topology and addressing scheme before you can configure IPv6 on the various nodes in your network.	"Creating a Numbering Scheme for Subnets" on page 93
6. Design a plan for tunnel usage.	Determine which routers should run tunnels to other subnets or external networks.	"Planning for Tunnels in the Network Topology" on page 91
7. Create an addressing plan for entities on the network.	Your plan for addressing servers, routers, and hosts should be in place before IPv6 configuration.	"Creating an IPv6 Addressing Plan for Nodes" on page 94
8. Develop an IPv6 security policy.	Investigate IP Filter, IP security architecture (IPsec), Internet Key Exchange (IKE), and other Solaris security features as you develop an IPv6 security policy.	Part IV
9. (Optional) Set up a DMZ.	For security purposes, you need an addressing plan for the DMZ and its entities before you configure IPv6.	"Security Considerations for the IPv6 Implementation" on page 92
10. Enable the nodes to support IPv6.	Configure IPv6 on all routers and hosts.	"General IPv6 Network Configuration Tasks (Task Map)" on page 123
11. Turn on network services.	Make sure that existing servers can support IPv6.	"Major TCP/IP Administrative Tasks (Task Map)" on page 152
12. Update name servers for IPv6 support.	Make sure that DNS, NIS, and LDAP servers are updated with the new IPv6 addresses.	"Configuring Name Service Support for IPv6" on page 138

IPv6 Network Topology Scenario

The tasks throughout this chapter explain how to plan for IPv6 services on a typical enterprise network. The following figure shows the network that is referred to throughout the chapter. Your proposed IPv6 network might include some or all of the network links that are illustrated in this figure.

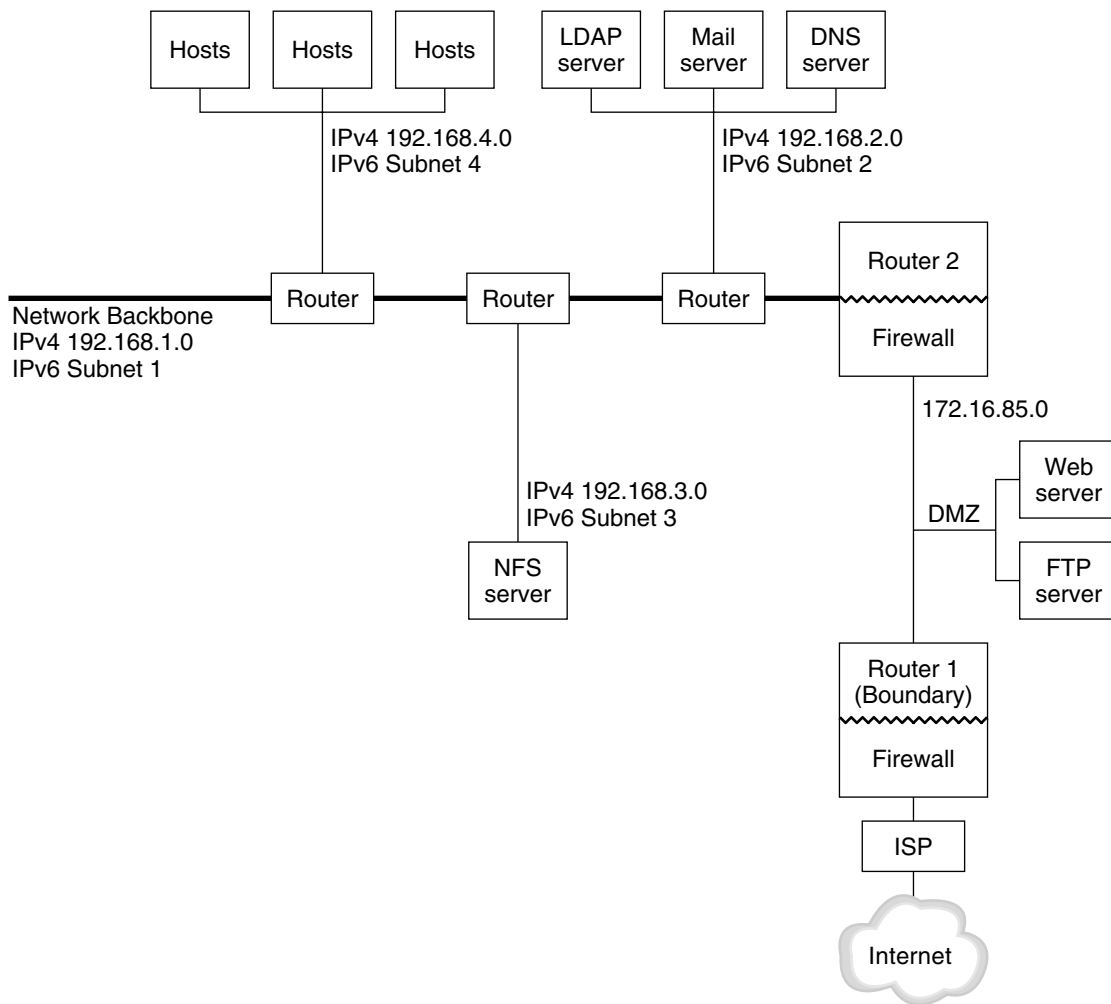


FIGURE 4-1 IPv6 Network Topology Scenario

The enterprise network scenario consists of five subnets with existing IPv4 addresses. The links of the network correspond directly to the administrative subnets. The four internal networks are shown with RFC 1918-style private IPv4 addresses, which is a common solution for the lack of IPv4 addresses. The addressing scheme of these internal networks follows:

- Subnet 1 is the internal network backbone 192.168.1.
- Subnet 2 is the internal network 192.168.2, with LDAP, sendmail, and DNS servers.
- Subnet 3 is the internal network 192.168.3, with the enterprise's NFS servers.
- Subnet 4 is the internal network 192.168.4, which contains hosts for the enterprise's employees.

The external, public network 172.16.85 functions as the corporation's DMZ. This network contains web servers, anonymous FTP servers, and other resources that the enterprise offers to the outside world. Router 2 runs a firewall and separates public network 172.16.85 from the internal backbone. On the other end of the DMZ, Router 1 runs a firewall and serves as the enterprise's boundary server.

In [Figure 4-1](#), the public DMZ has the RFC 1918 private address 172.16.85. In the real world, the public DMZ must have a registered IPv4 address. Most IPv4 sites use a combination of public addresses and RFC 1918 private addresses. However, when you introduce IPv6, the concept of public addresses and private addresses changes. Because IPv6 has a much larger address space, you use public IPv6 addresses on both private networks and public networks.

Preparing the Existing Network to Support IPv6

Note – The Solaris dual protocol stack supports concurrent IPv4 and IPv6 operations. You can successfully run IPv4-related operations during and after deployment of IPv6 on your network.

IPv6 introduces additional features to an existing network. Therefore, when you first deploy IPv6, you must ensure that you do not disrupt any operations that are working with IPv4. The subjects covered in this section describe how to introduce IPv6 to an existing network in a step-by-step fashion.

Preparing the Network Topology for IPv6 Support

The first step in IPv6 deployment is to assess which existing entities on your network can support IPv6. In most cases, the network topology-wires, routers, and hosts-can remain unchanged as you implement IPv6. However, you might have to prepare existing hardware and applications for IPv6 before actually configuring IPv6 addresses on network interfaces.

Verify which hardware on your network can be upgraded to IPv6. For example, check the manufacturers' documentation for IPv6 readiness regarding the following classes of hardware:

- Routers
- Firewalls
- Servers
- Switches

Note – All procedures in the this Part assume that your equipment, particularly routers, can be upgraded to IPv6.

Some router models cannot be upgraded to IPv6. For more information and a workaround, refer to [“IPv4 Router Cannot Be Upgraded to IPv6”](#) on page 179.

Preparing Network Services for IPv6 Support

The following typical IPv4 network services in the current Solaris release are IPv6 ready:

- `sendmail`
- NFS
- HTTP (Apache 2.x or Orion)
- DNS
- LDAP

The IMAP mail service is for IPv4 only.

Nodes that are configured for IPv6 can run IPv4 services. When you turn on IPv6, not all services accept IPv6 connections. Services that have been ported to IPv6 will accept a connection. Services that have not been ported to IPv6 continue to work with the IPv4 half of the protocol stack.

Some issues can arise after you upgrade services to IPv6. For details, see [“Problems After Upgrading Services to IPv6”](#) on page 179.

Preparing Servers for IPv6 Support

Because servers are considered IPv6 hosts, by default their IPv6 addresses are automatically configured by the Neighbor Discovery protocol. However, many servers have multiple network interface cards (NICs) that you might want to swap out for maintenance or replacement. When you replace one NIC, Neighbor Discovery automatically generates a new interface ID for that NIC. This behavior might not be acceptable for a particular server.

Therefore, consider manually configuring the interface ID portion of the IPv6 addresses for each interface of the server. For instructions, refer to [“How to Manually Configure a Link-Local Address” on page 147](#). Later, when you need to replace an existing NIC, the already configured IPv6 address is applied to the replacement NIC.

▼ How to Prepare Network Services for IPv6 Support

Steps 1. **Update the following network services to support IPv6:**

- Mail servers
- NIS servers
- NFS

Note – LDAP supports IPv6 without requiring IPv6-specific configuration tasks.

2. **Verify that your firewall hardware is IPv6 ready.**

Refer to the appropriate firewall-related documentation for instructions.

3. **Verify that other services on your network have been ported to IPv6.**

For more information, refer to marketing collateral and associated documentation for the software.

4. **If your site deploys the following services, make sure that you have taken the appropriate measures for these services:**

- Firewalls
Consider strengthening the policies that are in place for IPv4 to support IPv6. For more security considerations, see [“Security Considerations for the IPv6 Implementation” on page 92](#).
- Mail
In the MX records for DNS, consider adding the IPv6 address of your mail server.
- DNS

For DNS-specific considerations, see “How to Prepare DNS for IPv6 Support” on page 91.

- IPQoS

Use the same Diffserv policies on a host that were used for IPv4. For more information, see “Classifier Module” on page 758.

5. **Audit any network services that are offered by a node prior to converting that node to IPv6.**

▼ How to Prepare DNS for IPv6 Support

The current Solaris release supports DNS resolution on both the client side and the server side. Do the following to prepare DNS services for IPv6.

For more information that is related to DNS support for IPv6, refer to *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

- Steps**
1. **Ensure that the DNS server that performs recursive name resolution is dual-stacked (IPv4 and IPv6) or for IPv4 only.**
 2. **On the DNS server, populate the DNS database with relevant IPv6 database AAAA records in the forward zone.**

Note – Servers that run multiple critical services require special attention. Ensure that the network is working properly. Also ensure that all critical services are ported to IPv6. Then, add the server’s IPv6 address to the DNS database.

3. **Add the associated PTR records for the AAAA records into the reverse zone.**
4. **Add either IPv4 only data, or both IPv6 and IPv4 data into the NS record that describes zones.**

Planning for Tunnels in the Network Topology

The IPv6 implementation supports a number of tunnel configurations to serve as transition mechanisms as your network migrates to a mix of IPv4 and IPv6. Tunnels enable isolated IPv6 networks to communicate. Because most of the Internet runs IPv4, IPv6 packets from your site need to travel across the Internet through tunnels to destination IPv6 networks.

Here are some major scenarios for using tunnels in the IPv6 network topology:

- The ISP from which you purchase IPv6 service allows you to create a tunnel from your site’s boundary router to the ISP network. [Figure 4–1](#) shows such a tunnel. In such a case, you would run a manual, IPv6 over IPv4 tunnel.

- You manage a large, distributed network with IPv4 connectivity. To connect the distributed sites that use IPv6, you can run an automatic 6to4 tunnel from the edge router of each subnet.
- Sometimes, a router in your infrastructure cannot be upgraded to IPv6. In this case, you can create a manual tunnel over the IPv4 router, with two IPv6 routers as endpoints.

For procedures for configuring tunnels, refer to [“Tasks for Configuring Tunnels for IPv6 Support \(Task Map\)”](#) on page 129. For conceptual information regarding tunnels, refer to [“IPv6 Tunnels”](#) on page 233.

Security Considerations for the IPv6 Implementation

When you introduce IPv6 into an existing network, you must take care not to compromise the security of the site. Be aware of the following security issues as you phase in your IPv6 implementation:

- The same amount of filtering is required for both IPv6 packets and IPv4 packets.
- IPv6 packets are often tunneled through a firewall. Therefore, you should implement either of the following scenarios:
 - Have the firewall do content inspection inside the tunnel.
 - Put an IPv6 firewall with similar rules at the opposite tunnel endpoint.
- Some transition mechanisms exist that use IPv6 over UDP over IPv4 tunnels. These mechanisms might prove dangerous by short-circuiting the firewall.
- IPv6 nodes are globally reachable from outside the enterprise network. If your security policy prohibits public access, you must establish stricter rules for the firewall. For example, consider configuring a stateful firewall.

This book includes security features that can be used within an IPv6 implementation.

- The IP security architecture (IPsec) feature enables you to provide cryptographic protection for IPv6 packets. For more information, refer to [Chapter 18](#).
- The Internet Key Exchange (IKE) feature enables you to use public key authentication for IPv6 packets. For more information, refer to [Chapter 21](#).

Preparing an IPv6 Addressing Plan

A major part of the transition from IPv4 to IPv6 includes the development of an addressing plan. This task involves the following preparations:

- [“Obtaining a Site Prefix”](#) on page 93

- [“Creating the IPv6 Numbering Scheme” on page 93](#)

Obtaining a Site Prefix

Before you configure IPv6, you must obtain a site prefix. The site prefix is used to derive IPv6 addresses for all the nodes in your IPv6 implementation. For an introduction to site prefixes, refer to [“Prefixes in IPv6” on page 76](#).

Any ISP that supports IPv6 can provide your organization with a 48-bit IPv6 site prefix. If your current ISP only supports IPv4, you can use another ISP for IPv6 support while retaining your current ISP for IPv4 support. In such an instance, you can use one of several workarounds. For more information, see [“Current ISP Does Not Support IPv6” on page 179](#).

If your organization is an ISP, then you obtain site prefixes for your customers from the appropriate Internet registry. For more information, see the Internet Assigned Numbers Authority (IANA) (<http://www.iana.org>).

Creating the IPv6 Numbering Scheme

Unless your proposed IPv6 network is entirely new, use your existing IPv4 topology as the basis for the IPv6 numbering scheme.

Creating a Numbering Scheme for Subnets

Begin your numbering scheme by mapping your existing IPv4 subnets into equivalent IPv6 subnets. For example, consider the subnets illustrated in [Figure 4–1](#). Subnets 1–4 use the RFC 1918 IPv4 private address designation for the first 16 bits of their addresses, in addition to the digits 1–4 to indicate the subnet. For illustrative purposes, assume that the IPv6 prefix `2001:db8:3c4d/48` has been assigned to the site. The following table shows how the private IPv4 prefixes map into IPv6 prefixes.

IPv4 Subnet Prefix	Equivalent IPv6 Subnet Prefix
192.168.1.0/24	2001:db8:fd3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

Creating an IPv6 Addressing Plan for Nodes

For most hosts, stateless autoconfiguration of IPv6 addresses for their interfaces is an appropriate, time-saving strategy. When the host receives the site prefix from the nearest router, Neighbor Discovery automatically generates IPv6 addresses for each interface on the host.

Servers need to have stable IPv6 addresses. If you do not manually configure a server's IPv6 addresses, a new IPv6 address is autoconfigured whenever a NIC card is replaced on the server. Keep the following tips in mind when you create addresses for servers:

- Give servers meaningful and stable interface IDs. One strategy is to use a sequential numbering scheme for interface IDs. For example, the internal interface of the LDAP server in [Figure 4-1](#) might become `2001:db8:3c4d:2::2`.
- Alternatively, if you do not regularly renumber your IPv4 network, consider using the existing IPv4 addresses of the routers and servers as their interface IDs. In [Figure 4-1](#), suppose Router 1's interface to the DMZ has the IPv4 address `123.456.789.111`. You can convert the IPv4 address to hexadecimal and use the result as the interface ID. The new interface ID would be `::7bc8:156F`.

Only use this approach if you own the registered IPv4 address, rather than having obtained the address from an ISP. If you use an IPv4 address that was given to you by an ISP, you create a dependency that would create problems if you change ISPs.

Due to the limited number of IPv4 addresses, in the past a network designer had to consider where to use global, registered addresses and private, RFC 1918 addresses. However, the notion of global and private IPv4 addresses does not apply to IPv6 addresses. You can use global unicast addresses, which include the site prefix, on all links of the network, including the public DMZ.

Configuring TCP/IP Network Services and IPv4 Addressing (Tasks)

TCP/IP network administration evolves in two stages. The first stage is to assemble the hardware. Then, you configure the daemons, files, and services that implement the TCP/IP protocol.

This chapter explains how to configure TCP/IP on a network that implements IPv4 addressing and services.

Note – Many of the tasks in this chapter apply to both IPv4-only and IPv6-enabled networks. Where configuration tasks differ between the two addressing formats, the IPv4 configuration steps are in this chapter. The task in this chapter then cross references the equivalent IPv6 task in [Chapter 6](#).

This chapter contains the following information:

- “Before You Configure an IPv4 Network (Task Map)” on page 96
- “Determining Host Configuration Modes” on page 97
- “Adding a Subnet to a Network (Task Map)” on page 99
- “Network Configuration Procedures” on page 101
- “Network Configuration Task Map” on page 101
- “Monitoring and Modifying Transport Layer Services” on page 108
- “Administering Physical Interfaces” on page 112
- “Configuring a Router” on page 118
- “Multihomed Hosts” on page 121

Before You Configure an IPv4 Network (Task Map)

Before you configure TCP/IP, complete the tasks that are listed in the following table.

Task	Description	For Instructions
1. Design the network topology.	Determine the physical layout of the network.	"Network Topology Overview" on page 65.
2. Obtain a network number from your ISP or Regional Internet Registry (RIR).	Get a registered network number, which enables systems at your site to communicate externally.	"Designing Your IPv4 Addressing Scheme" on page 58.
3. Plan the IPv4 addressing scheme for the network. If applicable, include subnet addressing.	Use the network number as the basis for your addressing plan.	"Designing Your IPv4 Addressing Scheme" on page 58.
4. Assemble the network hardware depending on the network topology. Assure that the hardware is functioning properly.	Set up the systems, network media, routers, switches, hubs and bridges that you outlined in the network topology design.	The hardware manuals and "Network Topology Overview" on page 65.
5. Assign IPv4 addresses and host names to all systems in the network.	Assign the IPv4 addresses during Solaris OS installation or post-installation, in the appropriate files.	"Designing Your IPv4 Addressing Scheme" on page 58.
6. Run configuration software that is required by network interfaces and routers, if applicable.	Configure routers and multihomed hosts.	"Adding Routers to Your Network" on page 64 and "Configuring a Router" on page 118 for information on routers.
7. Determine which name service or directory service your network uses: NIS, LDAP, DNS, or local files.	Configure your selected name service and/or directory service.	<i>System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP).</i>
8. Select domain names for your network, if applicable.	Choose a domain name for your network and register it with the InterNIC.	<i>System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)</i>

Determining Host Configuration Modes

As a network administrator, you configure TCP/IP to run on hosts and routers (if applicable). You can configure these systems to obtain configuration information from files on the local system or from files that are located on other systems on the network. You need the following configuration information:

- Host name of each system
- IP address of each system
- Domain name to which each system belongs
- Default router
- IPv4 netmask in use on each system's network

A system that obtains TCP/IP configuration information from local files operates in *local files mode*. A system that obtains TCP/IP configuration information from a remote network server operates in *network client mode*.

Systems That Should Run in Local Files Mode

To run in local files mode, a system must have local copies of the TCP/IP configuration files. These files are described in [“TCP/IP Configuration Files” on page 183](#). The system should have its own disk, though this recommendation is not strictly necessary.

Most servers should run in local files mode. This requirement includes the following servers:

- Network configuration servers
- NFS servers
- Name servers that supply NIS, LDAP, or DNS services
- Mail servers

Additionally, routers should run in local files mode.

Systems that function exclusively as print servers do not need to run in local files mode. Whether individual hosts should run in local files mode depends on the size of your network.

If you are running a very small network, the amount of work that is involved in maintaining these files on individual hosts is manageable. If your network serves hundreds of hosts, the task becomes difficult, even with the network divided into a number of administrative subdomains. Thus, for large networks, using local files mode is usually less efficient. However, because routers and servers must be self-sufficient, they should be configured in local files mode.

Network Configuration Servers

Network configuration servers are the servers that supply the TCP/IP configuration information to hosts that are configured in network client mode. These servers support three booting protocols:

- RARP – Reverse Address Resolution Protocol (RARP) maps Ethernet addresses (48 bits) to IPv4 addresses (32 bits), which is the reverse of ARP. When you run RARP on a network configuration server, hosts that are running in network client mode obtain their IP addresses and TCP/IP configuration files from the server. The `in.rarpd` daemon enables RARP services. Refer to the `in.rarpd(1M)` man page for details.
- TFTP – The Trivial File Transfer Protocol (TFTP) is an application that transfers files between remote systems. The `in.tftpd` daemon executes TFTP services, enabling file transfer between network configuration servers and their network clients. Refer to the `in.tftpd(1M)` man page for details.
- Bootparams – The Bootparams protocol supplies parameters for booting that are required by clients that boot off the network. The `rpc.bootparamd` daemon executes these services. Refer to the `bootparamd(1M)` man page for details.

Network configuration servers can also function as NFS file servers.

If you are configuring any hosts as network clients, then you must also configure at least one system on your network as a network configuration server. If your network is subnetted, then you must have at least one network configuration server for each subnet with network clients.

Systems That Are Network Clients

Any host that obtains its configuration information from a network configuration server operates in network client mode. Systems that are configured as network clients do not require local copies of the TCP/IP configuration files.

Network client mode simplifies administration of large networks. Network client mode minimizes the number of configuration tasks that you perform on individual hosts. Network client mode assures that all systems on the network adhere to the same configuration standards.

You can configure network client mode on all types of computers. For example, you can configure network client mode on fully standalone systems or dataless systems.

Mixed Configurations

Configurations are not limited to either an all-local-files mode or an all-network-client mode. Routers and servers should always be configured in local mode. For hosts, you can use any combination of local files and network client mode.

IPv4 Network Topology Scenario

Figure 5-1 shows the hosts of a fictitious network with the network number 192.9.200. The network has one network configuration server, which is called `sahara`. Hosts `tenere` and `nubian` have their own disks and run in local files mode. Host `faiyum` also has a disk, but this system operates in network client mode.

Finally, the system `timbuktu` is configured as a router. The system includes two network interfaces. The first interface is named `timbuktu`. This interface belongs to network 192.9.200. The second interface is named `timbuktu-201`. This interface belongs to network 192.9.201. Both networks are in the organizational domain `deserts.worldwide.com`. The domain uses local files as its name service.

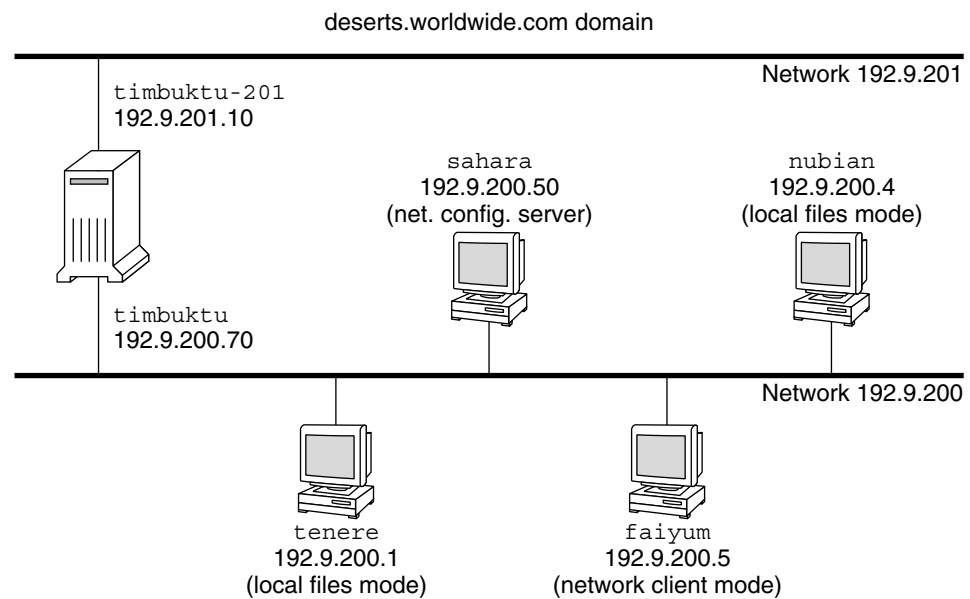


FIGURE 5-1 Hosts in an IPv4 Network Topology Scenario

Adding a Subnet to a Network (Task Map)

If you are changing from a network that does not use a subnet to a network that does use a subnet, perform the tasks in the following task map.

Note – The information in this section applies to IPv4 subnets only. For information on planning IPv6 subnets, refer to [“Preparing the Network Topology for IPv6 Support”](#) on page 89 and [“Creating a Numbering Scheme for Subnets”](#) on page 93.

Task	Description	For Instructions
1. Determine if your network topology requires subnets.	Decide on the new subnet topology, including where to locate routers and hosts on the subnets.	“Adding Routers to Your Network” on page 64, “What Is Subnetting?” on page 189, and “Network Classes” on page 202
2. Assign the IP addresses with the new subnet number to the systems to become members of the subnet.	Configure IP addresses that use the new subnet number, either during Solaris OS installation or later, in the <code>/etc/hostname.interface</code> file.	“Deciding on an IP Addressing Format for Your Network” on page 54
3. Configure the network mask of the subnet on all prospective systems in the subnet.	Modify the <code>/etc/inet/netmasks</code> file, if you are manually configuring network clients. Or, supply the netmask to the Solaris installation program.	“netmasks Database” on page 188 and “Creating the Network Mask for IPv4 Addresses” on page 189
4. Edit the network databases with the new IP addresses of all systems in the subnet.	Modify the <code>/etc/inet/hosts</code> and <code>/etc/inet/ipnodes</code> files on all hosts to reflect the new host addresses.	“hosts Database” on page 185
5. Reboot all systems.		

Network Configuration Task Map

Task	Description	For Instructions
Configure a host for local files mode	Involves editing the <code>nodename</code> , <code>hostname</code> , <code>hosts</code> , <code>defaultdomain</code> , <code>defaultrouter</code> , and <code>netmasks</code> files	“How to Configure a Host for Local Files Mode” on page 102
Set up a network configuration server	Involves turning on the <code>in.tftpd</code> daemon, and editing the <code>hosts</code> , <code>ethers</code> , and <code>bootparams</code> files	“How to Set Up a Network Configuration Server” on page 104
Configure a host for network client mode	Involves creating the <code>hostname</code> file, editing the <code>hosts</code> file, and deleting the <code>nodename</code> and <code>defaultdomain</code> files, if they exist	“How to Configure Hosts for Network Client Mode” on page 105
Specify a routing strategy for the network client	Involves determining whether to use static routing or dynamic routing on the host.	“How to Enable Static Routing on a Network Client” on page 106 and “How to Enable Dynamic Routing on a Network Client” on page 107.

Network Configuration Procedures

Network software installation occurs along with the installation of the operating system software. At that time, certain IP configuration parameters must be stored in appropriate files so that they can be read at boot time.

The network configuration process involves creating or editing the network configuration files. How configuration information is made available to a system’s kernel is conditional. The availability depends on whether these files are stored locally (local files mode) or acquired from the network configuration server (network client mode).

The parameters that are supplied during network configuration follow:

- The IP address of each network interface on every system.

- The host names of each system on the network. You can type the host name in a local file or a name service database.
- The NIS, LDAP, or DNS domain name in which the system resides, if applicable.
- The default router addresses. You supply this information if you have a simple network topology with only one router attached to each network. You also supply this information if your routers do not run routing protocols such as the Router Discovery Server Protocol (RDISC) or the Router Information Protocol (RIP). See [“Routing Protocols in the Solaris OS” on page 201](#) for more information about these protocols.
- Subnet mask (required only for networks with subnets).

If the Solaris installation program detects more one interface on the system, you can optionally configure the additional interfaces during installation. For complete instructions, see *Solaris 10 Installation Guide: Basic Installations*.

This chapter contains information on creating and editing local configuration files. See *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* for information on working with name service databases.

▼ How to Configure a Host for Local Files Mode

Use this procedure for configuring TCP/IP on a host that runs in local files mode.

Steps 1. Assume the Primary Administrator role, or become superuser

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Change to the `/etc` directory.

3. Type the host name of the system in the `/etc/nodename` file.

For example, if the name of the host is `tenere`, type `tenere` in the file.

4. Verify that a file called `/etc/hostname.interface` for each network interface on the system.

`interface` is the name of the interface, such as `eri`, plus a number, for example, `eri0`. You should have at least one `/etc/hostname.interface0` file, representing the primary network interface.

The Solaris installation program automatically creates this file for the primary network interface and, if applicable, any additional interfaces that were configured during installation. You do not need to configure additional interfaces at boot time. However, if you later want to use an interface that was not configured at boot time, you need to manually configure that interface.

For steps for manually configuring interfaces, refer to “Administering Physical Interfaces” on page 112.

5. **Type either the interface IP address or the interface name in each `/etc/hostname.interface` file.**

The first line of `/etc/hostname.interface` can have either the IP address of the interface or a host name to be associated with the interface.

6. **Edit the `/etc/inet/hosts` file.**

- a. **Add the IP addresses that you have assigned to any additional network interfaces in the local host along with the corresponding host name for each interface.**

The Solaris installation program has already created entries for the primary network interface, loopback address, and, if applicable, any additional interfaces that were configured during installation.

- b. **Add the IP address or addresses of the file server, if the `/usr` file system is NFS mounted.**

7. **Type the host’s fully qualified domain name in the `/etc/defaultdomain` file.**

For example, suppose host `tenere` was part of the domain `deserts.worldwide.com`. Therefore, you would type `deserts.worldwide.com` in `/etc/defaultdomain`. See “`/etc/defaultdomain` File” on page 185 for more information.

8. **Type the router’s name in the `/etc/defaultrouter` file.**

See “`/etc/defaultrouter` File” on page 185 for information about this file.

9. **Type the name of the default router and its IP addresses in the `/etc/inet/hosts` file.**

Additional routing options are available, as discussed in “How to Configure Hosts for Network Client Mode” on page 105. You can apply these options to a local files mode configuration.

10. **Add the network mask for your network, if applicable:**

- If the host gets its IP address from a DHCP server, you do not have to specify the network mask.
- If you have set up a NIS server on the same network as this client, you can type `netmask` information in the appropriate database on the server.
- For all other conditions, do the following:

- a. **Type the network number and the netmask in the file `/etc/inet/netmasks`.**

Use the following format:

```
network-number netmask
```

For example, for the Class C network number 192.168.83, you would type:

```
192.168.83.0 255.255.255.0
```

For CIDR addresses, convert the network prefix into the equivalent dotted decimal representation. Network prefixes and their dotted decimal equivalents can be found in [Table 2-3](#). For example, use the following to express the CIDR network prefix 192.168.3.0/22.

```
192.168.3.0 255.255.252.0
```

- b. Change the lookup order for netmasks in `/etc/nsswitch.conf`, so that local files are searched first:**

```
netmasks:  files nis
```

- 11. Reboot each system on the network.**

▼ How to Set Up a Network Configuration Server

Information for setting up installation servers and boot servers is found in *Solaris 10 Installation Guide: Basic Installations*.

- Steps**
- 1. Assume the Primary Administrator role, or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

- 2. Change to the root (/) directory of the prospective network configuration server.**

- 3. Turn on the `in.tftpd` daemon by creating the directory `/tftpboot`:**

```
# mkdir /tftpboot
```

This command configures the system as a TFTP, bootparams, and RARP server.

- 4. Create a symbolic link to the directory.**

```
# ln -s /tftpboot/. /tftpboot/tftpboot
```

- 5. Enable the `tftp` line in the `/etc/inetd.conf` file.**

Check that the entry reads as follows:

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

This line prevents `in.tftpd` from retrieving any file other than the files that are located in `/tftpboot`.

- 6. Edit the `hosts` database, and add the host names and IP addresses for every client on the network.**

7. Edit the `ethers` database, and create entries for every host on the network that runs in network client mode.

8. Edit the `bootparams` database.

See “[bootparams Database](#)” on page 197. Use the wildcard entry or create an entry for every host that runs in network client mode.

9. Convert the `/etc/inetd.conf` entry into a Service Management Facility (SMF) service manifest, and enable the resulting service:

```
# /usr/sbin/inetconv
```

10. Verify that `in.tftpd` is working correctly.

```
# svcs network/tftp/udp6
```

You should receive output resembling the following:

```
STATE          STIME      FMRI
online         18:22:21  svc:/network/tftp/udp6:default
```

More Information

Administering the `in.tftpd` Daemon

The `in.tftpd` daemon is managed by the Service Management Facility. Administrative actions on `in.tftpd`, such as enabling, disabling, or restarting, can be performed using the `svcadm` command. Responsibility for initiating and restarting this service is delegated to `inetd`. Use the `inetadm` command to make configuration changes and to view configuration information for `in.tftpd`. You can query the service’s status by using the `svcs` command. For an overview of the Service Management Facility, refer to Chapter 9, “Managing Services (Overview),” in *System Administration Guide: Basic Administration*.

Configuring Network Clients

Network clients receive their configuration information from network configuration servers. Therefore, before you configure a host as a network client you must ensure that at least one network configuration server is set up for the network.

▼ How to Configure Hosts for Network Client Mode

Do the following procedure on each host to be configured in network client mode.

Steps 1. Assume the Primary Administrator role, or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic*

Administration.

2. Search the `/etc` directory for the `nodename` file.

If such a file exists, delete it.

Eliminating `/etc/nodename` causes the system to use the `hostconfig` program to obtain the host name, domain name, and router addresses from the network configuration server. See [“Network Configuration Procedures”](#) on page 101.

3. Create the `/etc/hostname.interface` file, if it does not exist.

Ensure that the file is empty. An empty `/etc/hostname.interface` file causes the system to acquire the IP address from the network configuration server.

4. Ensure that the `/etc/inet/hosts` file contains only the host name and IP address of the loopback network interface.

```
# cat /etc/inet/hosts
# Internet host table
#
127.0.0.1      localhost
```

The IPv4 loopback interface has the IP address `127.0.0.1`.

For more information, see [“Loopback Address”](#) on page 186. The file should not contain the IP address and host name for the local host (primary network interface).

5. Check for the existence of an `/etc/defaultdomain` file.

If such a file exists, delete it.

The `hostconfig` program automatically sets the domain name. To override the domain name that is set by `hostconfig`, type the substitute domain name in the `/etc/defaultdomain` file.

6. Ensure that the search paths in the client’s `/etc/nsswitch.conf` file reflect the name service requirements for your network.

▼ How to Enable Static Routing on a Network Client

This procedure enables static routing on a network client. Clients that use static routing do not run any dynamic routing protocol. If you supplied the name of a default router when installing Solaris OS on a client, then that client is already configured to use static routing. For more information on static routing, refer to [“Configuring a Router”](#) on page 118.

Steps 1. On the network client, assume the Primary Administrator role, or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, [“Working With the Solaris Management Console \(Tasks\),”](#) in *System Administration Guide: Basic*

Administration.

2. **Create the `/etc/defaultrouter` file.**
3. **Add an entry for a router on the network into the `/etc/defaultrouter` file.**

```
# cat /etc/defaultrouter
192.168.45.2
192.168.47.55
```

In this example, routers 192.168.45.2 and 192.168.47.55 are configured as the default routers for the local host. See [“`/etc/defaultrouter` File” on page 185](#). Two static default routes are then installed in the routing table.

▼ How to Enable Dynamic Routing on a Network Client

If you supplied the name of a default router when installing Solaris OS on a client, then that client is configured to use static routing. Clients that use dynamic routing run the routing protocols in the `in.routed` daemon. Use the next procedure to enable dynamic routing on the network client. For more information on dynamic routing, refer to [“Configuring a Router” on page 118](#).

- Steps**
1. **On the network client, assume the Primary Administrator role, or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **If you do not want static default routes, delete the `/etc/defaultrouter` file.**
An empty `/etc/defaultrouter` file forces a network client to use dynamic routing
3. **Enable routing protocols on the network client.**

```
# routeadm -e ipv4-routing
routeadm -u
```

Now IPv4 dynamic routing is enabled, and the `in.routed` daemon discovers default route by using the RDISC protocol.

Monitoring and Modifying Transport Layer Services

The transport layer protocols TCP, SCTP, and UDP are part of the standard Solaris OS package. These protocols typically need no intervention to run properly. However, circumstances at your site might require you to log or modify services that run over the transport layer protocols. Then, you must modify the profiles for these services by using the Service Management Facility (SMF), which is described in Chapter 9, “Managing Services (Overview),” in *System Administration Guide: Basic Administration*.

The `inetd` daemon is responsible for starting standard Internet services when a system boots. These services include applications that use TCP, SCTP, or UDP as their transport layer protocol. You can modify existing Internet services or add new services using the SMF commands. For more information about `inetd`, refer to “[inetd Internet Services Daemon](#)” on page 192.

Operations that involve the transport layer protocols include:

- Logging of all incoming TCP connections
- Adding services that run over a transport layer protocol, using SCTP as an example
- Configuring the TCP wrappers facility for access control

For detailed information on the `inetd` daemon refer to the `inetd(1M)` man page.

▼ How to Log the IP Addresses of All Incoming TCP Connections

- Steps**
1. **On the local system, assume the Network Management role or become superuser.**

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Set TCP tracing to enabled for all services managed by `inetd`.**

```
# inetadm -M tcp_trace=TRUE
```

▼ How to Add Services That Use the SCTP Protocol

The SCTP transport protocol provides services to application layer protocols in a fashion similar to TCP. However, SCTP enables communication between two systems, either or both of which can be multihomed. The SCTP connection is called an *association*. In an association, an application divides the data to be transmitted into one or more message streams, or *multi-streamed*. An SCTP connection can go to endpoints with multiple IP addresses, which is particularly important for telephony applications. The multihoming capabilities of SCTP are a security consideration if your site uses IP Filter or IPsec. Some of these considerations are described in the `sctp(7P)` man page.

By default, SCTP is included in the Solaris OS and does not require additional configuration. However, you might need to explicitly configure certain application layer services to use SCTP. Some example applications are `echo` and `discard`. The next procedure shows how to add an echo service that uses an SCTP one-to-one style socket.

Note – You can also use the following procedure to add services for the TCP and UDP transport layer protocols.

The following task shows how to add an SCTP `inet` service that is managed by the `inetd` daemon to the SMF repository. The task then shows how to use the Service Management Facility (SMF) commands to add the service.

- For information about SMF commands, refer to “SMF Command-Line Administrative Utilities” in *System Administration Guide: Basic Administration*.
- For syntactical information, refer to the man pages for the SMF commands, as cited in the procedure.
- For detailed information about SMF refer to the `smf(5)` man page.

Before You Begin Before you perform the following procedure, create a manifest file for the service. The procedure uses as an example a manifest for the `echo` service that is called `echo.sctp.xml`.

Steps 1. **Log in to the local system with a user account that has write privileges for system files.**

2. **Edit the `/etc/services` file and add a definition for the new service.**

Use the following syntax for the service definition.

```
service-name | port/protocol | aliases
```

3. **Add the new service.**

Go to the directory where the service manifest is stored and type the following:

```
# cd dir-name
# svccfg import service-manifest-name
```

For a complete syntax of `svccfg`, refer to the `svccfg(1M)` man page.

Suppose you want to add a new SCTP `echo` service using the manifest `echo.sctp.xml` that is currently located in the `service.dir` directory. You would type the following:

```
# cd service.dir
# svccfg import echo.sctp.xml
```

4. Verify that the service manifest has been added:

```
# svcs FMRI
```

For the `FMRI` argument, use the Fault Managed Resource Identifier (FMRI) of the service manifest. For example, for the SCTP `echo` service, you would use the following command:

```
# svcs svc:/network/echo:sctp_stream
```

Your output should resemble the following:

```
STATE          STIME          FMRI
disabled       16:17:00      svc:/network/echo:sctp_stream
```

For detailed information about the `svcs` command, refer to the `svcs(1)` man page.

The output indicates that the new service manifest is currently disabled.

5. List the properties of the service to determine if you must make modifications.

```
# inetadm -l FMRI
```

For detailed information about the `inetadm` command, refer to the `inetadm(1M)` man page.

For example, for the SCTP `echo` service, you would type the following:

```
# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE
           name="echo"
           endpoint_type="stream"
           proto="sctp"
           isrpc=FALSE
           wait=FALSE
           exec="/usr/lib/inet/in.echod -s"
           .
           .
           default tcp_trace=FALSE
           default tcp_wrappers=FALSE
```

6. Enable the new service:

```
# inetadm -e FMRI
```

7. Verify that the service is enabled:

For example, for the new echo service, you would type the following:

```
# inetadm | grep sctp_stream
.
.
enabled online svc:/network/echo:sctp_stream
```

Example 5–1 Adding a Service That Uses the SCTP Transport Protocol

The following example shows the commands to use and the file entries required to have the echo service use the SCTP transport layer protocol.

```
$ cat /etc/services
.
.
echo          7/tcp
echo          7/udp
echo          7/sctp

# cd service.dir

# svccfg import echo.sctp.xml

# svcs network/echo*
STATE      STIME      FMRI
disabled   15:46:44   svc:/network/echo:dgram
disabled   15:46:44   svc:/network/echo:stream
disabled   16:17:00   svc:/network/echo:sctp_stream

# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE
           name="echo"
           endpoint_type="stream"
           proto="sctp"
           isrpc=FALSE
           wait=FALSE
           exec="/usr/lib/inet/in.echod -s"
           user="root"
default    bind_addr=""
default    bind_fail_max=-1
default    bind_fail_interval=-1
default    max_con_rate=-1
default    max_copies=-1
default    con_rate_offline=-1
default    failrate_cnt=40
default    failrate_interval=60
default    inherit_env=TRUE
default    tcp_trace=FALSE
default    tcp_wrappers=FALSE

# inetadm -e svc:/network/echo:sctp_stream

# inetadm | grep echo
disabled disabled svc:/network/echo:stream
```

```
disabled disabled      svc:/network/echo:dgram
enabled  online        svc:/network/echo:sctp_stream
```

▼ How to Use TCP Wrappers to Control Access to TCP Services

The `tcpd` program implements *TCP wrappers*. TCP wrappers add a measure of security for service daemons such as `ftpd` by standing between the daemon and incoming service requests. TCP wrappers log successful and unsuccessful connection attempts. Additionally, TCP wrappers can provide access control, allowing or denying the connection depending on where the request originates. You can use TCP wrappers to protect daemons such as SSH, Telnet, and FTP. The `sendmail` application can also use TCP wrappers, as described in “Support for TCP Wrappers From Version 8.12 of `sendmail`” in *System Administration Guide: Network Services*.

- Steps**
1. **On the local system, assume the Primary Administrator role, or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Set TCP wrappers to enabled.**

```
# inetadm -M tcp_wrappers=TRUE
```

3. **Configure the TCP wrappers access control policy as described in the `hosts_access(3)` man page.**

This man page can be found in the `/usr/sfw/man` directory on the SFW CD-ROM, which is packaged along with the Solaris OS CD-ROM.

Administering Physical Interfaces

A Solaris OS-based system usually has two types of interfaces, physical and logical. *Physical interfaces* consist of a driver and a connector into which you plug network media, such as an Ethernet cable. *Logical interfaces* are logically configured onto existing physical interfaces, such as interfaces that are configured for tunnels or configured with IPv6 addresses. This section describes how to configure physical interfaces after installation. Instructions for configuring logical interfaces are included with tasks for features that require logical interfaces, for example, “How to Manually Configure IPv6 Over IPv4 Tunnels” on page 130.

This section contains the following tasks for administering physical interfaces:

- Adding physical interfaces after system installation
- Adding a virtual local area network (VLAN) to a network adapter

Administering the Physical Interface

Types of physical interfaces include interfaces that are built into the system and separately purchased interfaces. Each interface resides on a *network interface card* (NIC).

Built-in NICs are present on the system when it is purchased. An example of an interface on a built-in NIC is the *primary network interface*, such as `eri0` or `hme0`. You must configure the system's primary network interface at installation time.

NICs such as `eri` and `hme` have only one interface. However, many brands of NICs have multiple interfaces. A multiple interface NIC such as the `qfe` card has four interfaces, `qfe0` – `qfe3`. The Solaris installation program detects all interfaces present at installation and asks if you want to configure the interfaces. You can configure these interfaces at boot time or at a later date.

Note – NICs are also referred to as *network adapters*.

In addition to the built-in NICs, you can add separately purchased NICs to a system. You physically install a separately purchased NIC according to the manufacturer's instructions. Then, you need to configure the interfaces on the NIC so that the interfaces can be used for passing data traffic.

The following are reasons to configure additional interfaces on a system after installation:

- You want to upgrade the system to become a multihomed host. For more information about multihomed hosts, refer to [“Multihomed Hosts” on page 121](#).
- You want to change the host to a router. For instructions on configuring routers, refer to [“Configuring a Router” on page 118](#).
- You want to add an interface to an IPMP group. For information about interfaces in an IPMP group, refer to [“IPMP Interface Configurations” on page 644](#).

▼ How to Add a Physical Interface After Installation

Before You Begin

Determine the IPv4 addresses that you want to use for the additional interfaces.

The physical interface to be configured must be present on the system. For information on installing separately purchased NIC hardware, refer to the manufacturer's instructions that accompany the NIC.

- Steps** 1. **On the system with the interfaces to be configured, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Create an `/etc/hostname.interface` file for each interface to be configured.**

For example, to add a `qfe0` interface, you would create the following file:

```
# cat /etc/hostname.qfe0
```

3. **Edit the `/etc/hostname.interface` file, and add the IP address of the interface.**

4. **Add entries for the new interfaces to the `/etc/inet/hosts` file.**

5. **Configure each interface as “up.”**

Use the `ifconfig` command with the following syntax to plumb the interface:

```
# ifconfig interface plumb up
```

For example, for `qfe0` you would type:

```
# ifconfig qfe0 plumb up
```

6. **Reboot the system, using the `boot -r` command.**

7. **Verify that the newly configured interfaces are “up.”**

```
# ifconfig -a
```

The status line after each interface name reports if the interface is up:

```
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
```

Example 5–2 Configuring an Interface After System Installation

The following example shows how to add two interfaces, `qfe0` and `qfe1`. These interfaces are attached to the same network as the primary network interface, `hme0`.

```
#vi /etc/hostname.qfe0
10.0.0.32
# vi /etc/hostname.qfe1
10.0.0.33
# vi /etc/inet/hosts
# Internet host table
#
127.0.0.1      localhost
10.0.0.14     myhost
10.0.0.32     interface-2
10.0.0.33     interface-3

# ifconfig qfe0 plumb up
# ifconfig qfe1 plumb up
```

At this point, you would reboot the system. After the system comes up, you would verify the interface configuration.

```
ifconfig -a
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.14 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:c1:8b:c3
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 10.0.0.32 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:c8:f4:1d
qfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 4
    inet 10.0.0.33 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:c8:f4:1e
```

- See Also**
- To configure an IPv6 address onto an interface, refer to [“How to Manually Configure Interfaces for IPv6”](#) on page 128.
 - To set up failover detection and failback for interfaces using Network Multipathing (IPMP), refer to [Chapter 30](#).

▼ How to Remove a Physical Interface

- Steps**
1. **On the system with the interface to be removed, assume the Primary Administrator role, or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Remove the physical interface.**

Use the following form of the `ifconfig` command:

```
# ifconfig interface unplumb down
```

For example, you would remove the interface `eri1` as follows:

```
# ifconfig eri1 unplumb down
```

Configuring VLANs

Virtual local area networks (VLANs) are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of work groups, and to enforce security policies among each logical segment. With multiple VLANs on an adapter, a server with a single adapter can have a logical presence on multiple IP subnets. By default, 512 VLANs can be defined for each VLAN-aware adapter on your server.

If your network does not require multiple VLANs, you can use the default configuration, in which case no further configuration is necessary.

VLANs can be created according to various criteria, but each VLAN must be assigned a VLAN tag or VLAN ID (VID). The VID is a 12-bit identifier between 1 and 4094 that identifies a unique VLAN. For each network interface (for example, `ce0`, `ce1`, `ce2`, and so on; or `bge0`, `bge1`, `bge2`, and so on), 512 possible VLANs can be created. Because IP subnets are commonly used, use IP subnets when setting up a VLAN network interface. This means that each VID assigned to a VLAN interface of a physical network interface belongs to different subnets.

Tagging an Ethernet frame requires the addition of a tag header to the frame. The header is inserted immediately following the destination MAC address and the source MAC address. The tag header consists of two bytes of the Ethernet Tag Protocol Identifier (TPID, 0x8100) and two bytes of Tag Control Information (TCI). The following figure shows the Ethernet Tag Header format.

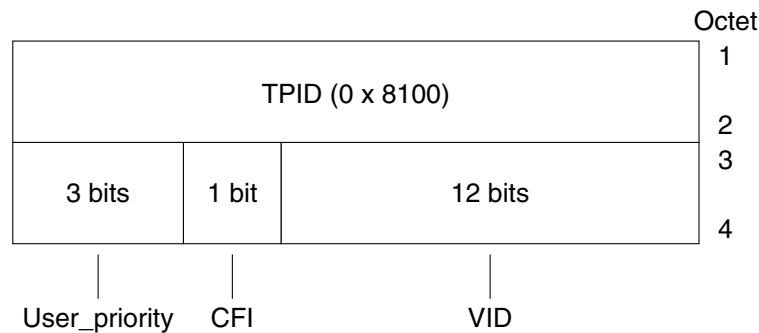


FIGURE 5-2 Ethernet Tag Header Format

▼ How To Configure Static VLANs

Steps 1. Assume the Primary Administrator role, or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Determine the type of interfaces in use on your system.

The network adapter on your system might not be referred to by the letters `ce`, which is required for a VLAN.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4>
mtu 8232 index 1
```

```

        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 2
        inet 129.156.200.77 netmask ffffffff00 broadcast
129.156.200.255

```

3. Create one `hostname.cenum` file (`hostname6.cenum` file for IPv6) for each VLAN that will be configured for each adapter on the server.

Use the following naming format that includes both the VID and the physical point of attachment (PPA):

VLAN logical PPA = $1000 * VID + Device PPA$ `ce123000` = $1000 * 123 + 0$

For example: `hostname.ce123000`

VLAN logical PPA = $1000 * VID + Device PPA$ `bge11000` = $1000 * 11 + 0$

For example: `hostname.bge11000`

This format limits the maximum number of PPAs (instances) you can configure to 1000 in the `/etc/path_to_inst` file.

For example, on a server with the Sun Gigabit Ethernet/P 3.0 adapter having an instance of 0, that belongs to two VLANs with VIDs 123 and 224, you would use `ce123000` and `ce224000`, respectively, as the two VLAN PPAs.

For a system containing a Broadcom Gigabit Ethernet adapter having an instance of 0, that belongs to two VLANs with VIDs 10 and 11, you would use `bge10000` and `bge11000`, respectively, as the two VLAN PPAs.

4. Configure a VLAN virtual device:

For example, you could use either of the following examples of `ifconfig`:

```

# ifconfig ce123000 plumb up
# ifconfig ce224000 plumb up

# ifconfig bge10000 plumb up# ifconfig bge11000 plumb up

```

The output of `ifconfig -a` on a system with VLAN devices `ce123000` and `ce224000` should resemble the following:

```

# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 129.144.131.91 netmask ffffffff00 broadcast 129.144.131.255
    ether 8:0:20:a4:4f:b8
ce123000: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 199.199.123.3 netmask ffffffff00 broadcast 199.199.123.255
    ether 8:0:20:a4:4f:b8
ce224000: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 4
    inet 199.199.224.3 netmask ffffffff00 broadcast 199.199.224.255
    ether 8:0:20:a4:4f:b8

```

The output of `ifconfig -a` on a system with VLAN devices `bge10000` and `bge11000` would resemble the following:

```

# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1

```

```
    inet 127.0.0.1 netmask ff000000
bge0: flags=1004843<UP,BROADCAST,RUNNING,MULTICAST,DHCP,IPv4> mtu 1500 index 2
    inet 129.156.205.172 netmask ffffffff broadcast 129.156.205.255
    ether 0:3:ba:29:f0:de
bge10000: flags=201000842<BROADCAST,RUNNING,MULTICAST,IPv4,CoS> mtu 1500 index
3
    inet 10.0.0.2 netmask ffffffff broadcast 10.0.0.255
    ether 0:3:ba:29:f0:de
bge11000: flags=201000842<BROADCAST,RUNNING,MULTICAST,IPv4,CoS> mtu 1500 index
4
    inet 10.0.1.2 netmask ffffffff broadcast 10.0.1.255
    ether 0:3:ba:29:f0:de
```

5. On the switch, set VLAN tagging and VLAN ports to coincide with the VLANs you have set up on the server.

Using the examples in Step 4, you would set up VLAN ports 123 and 224 on the switch or VLAN ports 10 and 11.

Refer to the documentation that came with your switch for specific instructions for setting VLAN tagging and ports.

Configuring a Router

A *router* is a system that fulfills the following requirements:

- Has at least two interfaces
- Forwards packets over the interfaces to destinations beyond the local link
- (Optional) Runs routing protocols

If one of the network interfaces is not disabled, the router automatically “talks” to the routing daemons. These daemons monitor routers on the network and advertise the router to the hosts on the network.

After the router is physically installed on the network, configure the router to operate in local files mode, as described in [“How to Configure a Host for Local Files Mode” on page 102](#). This configuration ensures that routers boot if the network configuration server is down. Remember that a router has a minimum of two interfaces to configure.

Because a router provides the interface between two or more networks, you must assign a unique name and IP address to each of the router’s physical network interfaces. Thus, each router has a host name and an IP address that are associated with its primary network interface, plus a minimum of one more unique name and an IP address for each additional network interface.

Note – You can configure all interfaces of a router during Solaris system installation. For instructions, *Solaris 10 Installation Guide: Basic Installations*.

▼ How to Configure an IPv4 Router

The following instructions assume that you are configuring interfaces for the router after installation.

You can use the following task to configure a system with only one physical interface (by default a host) to be a router. You might configure a single interface system as a router if it is to serve as one endpoint on a PPP link, as explained in *System Administration Guide: Network Services*.

Note – To configure an IPv6 router, refer to “[How to Configure an IPv6-Enabled Router](#)” on page 126

- Steps**
1. **On the system to be configured as a router, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Review which interfaces on the router were configured during installation.**

```
# ifconfig -a
```

The following command output of `ifconfig -a` shows that the interface `qfe0` was configured during installation. This interface is on the `172.16.0.0` network. The remaining interfaces on the `qfe` NIC, `qfe1 - qfe3`, have not been configured.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
qfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.16.26.232 netmask ffffffff broadcast 172.16.26.255
    ether 0:3:ba:11:b1:15
```

3. **Create an `/etc/hostname.interface` file for each additional physical interface to be configured.**

For example, you could create `hostname.qfe1` and `hostname.qfe2`. See “[/etc/hostname.interface File](#)” on page 184 for more information.

4. **Type the host name that you have defined for each `/etc/hostname.interface` file.**

For example, you could type the name `timbuktu` in the file `hostname.qfe1`. Then you could type the name `timbuktu-201` in the file `hostname.qfe2`.

5. Type the host name and IP address of each interface into the `/etc/inet/hosts` file.

For example:

```
172.16.26.232      deadsea          #interface for network 172.16.0.0
192.168.200.20    timbuktu        #interface for network 192.168.200
192.168.201.20    timbuktu-201    #interface for network 192.168.201
192.168.200.9     gobi
192.168.200.10    mojave
192.168.200.110   saltlake
192.168.200.12    chilean
```

The interfaces `timbuktu` and `timbuktu-201` are on the same system. Notice that the network address for `timbuktu-201` is different from that of `timbuktu`. The difference exists because the physical network media for network `192.168.201` is connected to the `timbuktu-201` network interface while the media for network `192.168.200` is connected to the `timbuktu` interface.

6. If the router is connected to any subnetted network, edit `/etc/inet/netmasks` as follows:

a. Type the network number and the netmask in the file `/etc/inet/netmasks`.

- For a network number such as `192.168.83.0`, you would type:

```
192.168.83.0    255.255.255.0
```

- For CIDR addresses, convert the network prefix into the equivalent dotted decimal representation. Network prefixes and their dotted decimal equivalents can be found in [Figure 2-2](#). For example, use the following to express the CIDR network prefix `192.168.3.0/22`.

```
192.168.3.0    255.255.252.0
```

b. Change the lookup order for netmasks in `/etc/nsswitch.conf` so that local files are searched first:

```
netmasks:    files nis dns
```

7. Enable packet forwarding on the router:

```
# routeadm -e ipv4-forwarding
# routeadm -u
```

At this point, the router can forward packets beyond the local network. The router also supports *static routing*, a process where you can manually add routes to the routing table. If you plan to use static routing on this system, then router configuration is complete.

8. (Optional) Start a routing protocol.

The routing daemon `/usr/sbin/in.routed` automatically updates the routing table, a process that is known as *dynamic routing*. Turn on the IPv4 routing protocols as follows:

```
# routeadm -e ipv4-routing
# routeadm -u
```

For syntax information on the `routeadm` command, see the `routeadm(1M)` man page.

Multihomed Hosts

In the Solaris OS, a system with more than one interface is considered a multihomed host. A multihomed host does not forward IP packets though you can configure the multihomed host to run routing protocols. You typically configure the following types of systems as multihomed hosts:

- NFS servers, particularly large data centers, can be attached to more than one network in order to share files among a large pool of users. These servers do not need to maintain routing tables.
- Database servers can have multiple network interfaces for the same reason as NFS servers, which is to provide resources to a large pool of users.
- Firewall gateways are systems that provide the connection between a company's network and public networks such as the Internet. Administrators set up firewalls as a security measure. When configured as a firewall, the host does not pass packets between the networks that are attached to the host's interfaces. However, the host can still provide standard TCP/IP services, such as `ftp` or `rlogin`, to authorized users.

▼ How to Create a Multihomed Host

- Steps**
1. **Assume the Primary Administrator role, or become superuser, on the prospective multihomed host.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, "Working With the Solaris Management Console (Tasks)," in *System Administration Guide: Basic Administration*.

2. **Create an `/etc/hostname.interface` file for each additional network interface that was not configured as part of the Solaris OS installation.**

Note – The Solaris installation program gives you the option of configuring all interfaces that are discovered during installation. If you chose this option, you should now have `/etc/hostname.interface` files for every interface that was configured during installation.

3. Verify that IP forwarding is not enabled on the multihomed host.

```
# routeadm
Configuration      Current           Current
      Option      Configuration    System State
-----
IPv4 forwarding    default (disabled) disabled
      IPv4 routing default (disabled) disabled
```

In the example above, both IP forwarding and routing are turned off. IP forwarding is disabled by default for a multihomed host.

4. Turn on dynamic routing for the multihomed host.

```
# routeadm -e ipv4-routing
# routeadm -u
```

Hosts should have dynamic routing enabled.

Configuring an IPv6 Network (Tasks)

This chapter contains tasks for configuring IPv6 on a network. The following major topics are covered:

- “General IPv6 Network Configuration Tasks (Task Map)” on page 123
- “Prerequisites for Configuring IPv6 on the Network” on page 125
- “Configuring an IPv6 Router” on page 125
- “Configuring Tunnels for IPv6 Support” on page 130
- “Configuring Name Service Support for IPv6” on page 138
- “Configuring IPv6 on a Host” on page 142
- “Configuring IPv6 on Servers” on page 147

For an overview of IPv6 concepts, refer to [Chapter 3](#). For IPv6 planning tasks, refer to [Chapter 4](#). To find reference information about the tasks in this chapter, refer to [Chapter 10](#).

General IPv6 Network Configuration Tasks (Task Map)

Perform the next tasks in the order that is shown in the table.

Task	Description	For Instructions
1. Ensure that you have completed the required prerequisites before you begin IPv6 configuration.	You must complete planning tasks and Solaris installation with IPv6 enabled before you configure an IPv6-enabled router.	“Prerequisites for Configuring IPv6 on the Network” on page 125

Task	Description	For Instructions
2. Configure a router.	Define the site prefix for the network. If needed, also configure interfaces for IPv6.	“How to Configure an IPv6-Enabled Router” on page 126
3. Configure tunnel interfaces on the router.	Set up a manual tunnel or a 6to4 tunnel interface on the router. The local IPv6 network needs tunnels to communicate with other, isolated IPv6 networks.	<ul style="list-style-type: none"> ■ “How to Configure a 6to4 Tunnel” on page 133 ■ “How to Manually Configure IPv6 Over IPv4 Tunnels” on page 130 ■ “How to Manually Configure IPv6 Over IPv6 Tunnels” on page 131 ■ “How to Configure IPv4 Over IPv6 Tunnels” on page 132
4. Configure the switches on the network.	If your network configuration includes switches, configure them for IPv6 at this point in the configuration process.	Refer to switch manufacturer’s documentation.
5. Configure any hubs on your network.	If your network configuration includes hubs, configure them for IPv6 at this point in the configuration process.	Refer to hub manufacturer’s documentation.
6. Configure the network name service for IPv6.	Configure your primary name service (DNS, NIS, or LDAP) to recognize IPv6 addresses after the router is configured for IPv6.	“How to Add IPv6 Addresses to DNS” on page 138 and “Adding IPv6 Addresses to NIS” on page 139
7. Configure IPv6 addresses for each host’s interface.	Enable address autoconfiguration for a host’s interfaces or manually configure the link-local address of the host with a token.	“How to Enable IPv6 Address Autoconfiguration” on page 142 or “How to Manually Configure a Link-Local Address” on page 147
8. (Optional) Set up a temporary address for a host.	Manually configure temporary interface IDs for hosts that need to keep their machine addresses secret.	“How to Configure a Temporary Address” on page 144
9. Configure static IPv6 addresses for all the servers’ interfaces	Manually configure the link-local IPv6 addresses for interfaces of servers. Most servers should have manually configured link-local addresses.	“How to Manually Configure a Link-Local Address” on page 147
Configure applications to support IPv6	Different applications might require different actions in order to support IPv6.	Refer to applications’ documentation

Prerequisites for Configuring IPv6 on the Network

Be sure that you have completed the following tasks before you configure IPv6 on the nodes to become part of the IPv6 network.

Task	For Information
1. Complete the planning tasks for the IPv6 network, such as upgrading hardware and software, and preparing an addressing plan.	“IPv6 Planning (Task Maps)” on page 85
2. Install the Solaris OS on each node.	<i>Solaris 10 Installation Guide: Basic Installations</i>
Note – Select the enable IPv6 option when you are prompted on the IPv6 screen during installation. If the node has multiple interfaces, select enable IPv6 when queried by the installation program, for all interfaces where you want to configure IPv6.	
3. (Optional) For nodes with multiple interfaces, you can configure additional interfaces for IPv6 while running the Solaris installation program.	<i>Solaris 10 Installation Guide: Basic Installations</i>

After you install the operating system, the following IPv6-related files and tables are in place:

- Each interface that you enabled for IPv6 during installation now has an associated `/etc/hostname6.interface` file, such as `hostname6.dmfe0`.
- The `/etc/inet/ipnodes` file is created. After installation, this file typically contains only the IPv6 and IPv4 loopback addresses.
- The `/etc/nsswitch.conf` file is modified to accommodate lookups using IPv6 addresses.
- The IPv6 address selection policy table is created. This table prioritizes the IP address format to use for transmissions over an IPv6-enabled interface.

Configuring an IPv6 Router

The first step in configuring IPv6 on a network is configuring IPv6 on a router. Router configuration involves a number of discrete tasks, which are described in this section. You might perform some or all of the tasks, depending on your site requirements.

▼ How to Configure an IPv6–Enabled Router

This procedure assumes that all interfaces of the router were configured for IPv6 during Solaris installation.

Steps 1. On the system that will become the IPv6 router, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Review which interfaces on the router were configured for IPv6 during installation.

```
# ifconfig -a
```

Check the output to ensure that the interfaces that you wanted to configure for IPv6 are now plumbed with link-local addresses. The following sample command output of `ifconfig -a` shows the IPv4 and IPv6 addresses that were configured for the router’s interfaces.

```
o0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.16.26.232 netmask ffffffff broadcast 172.16.26.255
    ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 172.16.26.220 netmask ffffffff broadcast 172.16.26.255
    ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
dmfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:11:b1:15
    inet6 fe80::203:baff:fe11:b115/10
dmfe1: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 3
    ether 0:3:ba:11:b1:16
    inet6 fe80::203:baff:fe11:b116/10
```

The output also shows that the primary network interface `dmfe0` and the additional interface `dmfe1` were configured during installation with the IPv6 link-local addresses `fe80::203:baff:fe11:b115/10` and `fe80::203:baff:fe11:b116/10`.

3. Configure IPv6 packet forwarding on all interfaces of the router.

```
# routeadm -e ipv6-forwarding
# routeadm -u
```

4. Start the routing daemon.

The `in.rripngd` daemon handles IPv6 routing. To start `in.rripngd`, type the following command.

```
# routeadm -e ipv6-routing
# routeadm -u
```

For syntax information on the `routeadm` command, see the `routeadm(1M)` man page.

5. Create the `/etc/inet/ndpd.conf` file.

You specify the site prefix to be advertised by the router and other configuration information in `/etc/inet/ndpd.conf`. This file is read by the `in.ndpd` daemon, which implements the IPv6 Neighbor Discovery protocol.

For a list of variables and allowable values, refer to [“`ndpd.conf` Configuration File” on page 211](#) and the `ndpd.conf(4)` man page.

6. Type the following text into the `/etc/inet/ndpd.conf` file:

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

This text tells the `in.ndpd` daemon to send out router advertisements over all interfaces of the router that are configured for IPv6.

7. Add additional text to the `/etc/inet/ndpd.conf` file to configure the site prefix on the various interfaces of the router.

The text should have the following format:

```
prefix global-routing-prefix:subnet ID/64 interface
```

The following sample `/etc/inet/ndpd.conf` file configures the router to advertise the site prefix `2001:0db8:3c4d::/48` over the interfaces `dmfe0` and `dmfe1`.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

```
if dmfe0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 dmfe0
```

```
if dmfe1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 dmfe1
```

8. Reboot the system.

The IPv6 router begins advertising on the local link any site prefix that is in the `ndpd.conf` file.

Example 6–1 `ifconfig` Output Showing IPv6 Interfaces

The following example shows output from the `ifconfig -a` command such as you would receive after you finish the [“Configuring an IPv6 Router” on page 125](#) procedure.

```
lo0: flags=1000849 <UP LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
```

```

dmfe0: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.16.15.232 netmask ffffffff broadcast 172.16.26.255
    ether 0:3:ba:11:b1:15
dmfe1: flags=1000843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 172.16.16.220 netmask ffffffff broadcast 172.16.26.255
    ether 0:3:ba:11:b1:16
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
dmfe0: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 2
    ether 0:3:ba:11:b1:15
    inet6 fe80::203:baff:fe11:b115/10
dmfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
    index 2
    inet6 2001:db8:3c4d:15:203:baff:fe11:b115/64
dmfe1: flags=2100841 <UP,RUNNING,MULTICAST,ROUTER,IPv6> mtu 1500 index 3
    ether 0:3:ba:11:b1:16
    inet6 fe80::203:baff:fe11:b116/10
dmfe1:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6> mtu 1500
    index 3
    inet6 2001:db8:3c4d:16:203:baff:fe11:b116/64

```

In this example, each interface that was configured for IPv6 now has two addresses. The entry with the name of the interface, such as `dmfe0`, shows the link-local address for that interface. The entry with the form *interface:n*, such as `dmfe0:1`, shows a global IPv6 address. This address includes the site prefix that you configured in the `/etc/ndpd.conf` file, in addition to the interface ID.

- See Also**
- To configure any tunnels from the routers that you have identified in your IPv6 network topology, refer to [“Configuring Tunnels for IPv6 Support”](#) on page 130.
 - For information about configuring switches and hubs on your network, refer to the manufacturer’s documentation.
 - To configure IPv6 hosts, refer to [“Configuring IPv6 on a Host”](#) on page 142.
 - To improve IPv6 support on servers, refer to [“Configuring IPv6 on Servers”](#) on page 147.
 - For detailed information about IPv6 commands, files, and daemons, refer to [“Solaris 10 IPv6 Implementation”](#) on page 211.

▼ How to Manually Configure Interfaces for IPv6

You can manually configure additional interfaces for IPv6 routers and multihomed hosts after Solaris installation.

- Steps**
1. **On the node with the interface to be configured for IPv6, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, *“Working With the Solaris Management Console (Tasks),”* in *System Administration Guide: Basic*

Administration.

2. Create empty `/etc/hostname6.interface` files for the interfaces that you want to configure for IPv6.

For example, suppose you want to configure interface `dmfe2` for IPv6. You then need to create the `/etc/hostname6.dmfe2` file.

3. Plumb the additional interfaces to be enabled for IPv6.

```
# ifconfig dmfe2 inet6 plumb up
```

For syntax information, refer to the `ifconfig(1M)` man page and “[ifconfig Command Extensions for IPv6 Support](#)” on page 219.

4. Take one of the following actions, depending on whether the system you are configuring is a router or multihomed host.

- If the interface is on a router, use the `routedm` command to enable routing and packet forwarding, as explained in “[How to Configure an IPv6-Enabled Router](#)” on page 126.
- If the interface is on a multihomed host, turn off routing and IP forwarding as follows:

```
# routedm -d ipv6-routing ipv6-forwarding
# routedm -d
# routedm -u
```

5. Reboot the system.

Tasks for Configuring Tunnels for IPv6 Support (Task Map)

Task	Description	For Instructions
Manually configure IPv6 over IPv4 tunnels.	Manually creates an IPv6 tunnel over a IPv4 network, a solution for reaching remote IPv6 networks within a larger, mostly IPv4 enterprise network.	“ How to Manually Configure IPv6 Over IPv4 Tunnels ” on page 130

Task	Description	For Instructions
Manually configure IPv6 over IPv6 tunnels.	Manually configures an IPv6 tunnel over an IPv6 network, typically used within a large enterprise network.	“How to Manually Configure IPv6 Over IPv6 Tunnels” on page 131
Manually configure IPv4 over IPv6 tunnels.	Manually configures an IPv4 tunnel over an IPv6 network, useful for large networks with both IPv4 and IPv6 networks.	“How to Configure IPv4 Over IPv6 Tunnels” on page 132
Automatically configure IPv6 over IPv4 tunnels (6to4 tunnels).	Create an automatic, 6to4 tunnel, a solution for reaching an external IPv6 site over the Internet.	“How to Configure a 6to4 Tunnel” on page 133
Configure a tunnel between a 6to4 router and a 6to4 relay router.	Enables a tunnel to a 6to4 relay router by using the <code>6to4relay</code> command.	“How to Configure a 6to4 Tunnel to a 6to4 Relay Router” on page 136

Configuring Tunnels for IPv6 Support

IPv6 networks are often isolated entities within the larger IPv4 world. Nodes on your IPv6 network might need to communicate with nodes on isolated IPv6 networks, either within your enterprise or remotely. Typically, you configure a tunnel between IPv6 routers, although IPv6 hosts can also function as tunnel endpoints. For tunnel planning information, refer to [“Planning for Tunnels in the Network Topology” on page 91](#).

You can set up automatically or manually configured tunnels for the IPv6 network. The Solaris IPv6 implementation supports the following types of tunnel encapsulation:

- IPv6 over IPv4 tunnels
- IPv6 over IPv6 tunnels
- IPv4 over IPv6 tunnels
- 6to4 tunnels

For conceptual descriptions of tunnels, see [“IPv6 Tunnels” on page 233](#).

▼ How to Manually Configure IPv6 Over IPv4 Tunnels

This procedure describes how to set up a tunnel from an IPv6 node to a remote IPv6 node over an IPv4 network.

Steps 1. **Log in to the local tunnel endpoint as Primary Administrator or as superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Create the `/etc/hostname6.ip.tunn` file.**

where *n* represents the tunnel number, beginning at zero for the first tunnel. Then, add entries by following these substeps:

a. **Add the tunnel source address and the tunnel destination address.**

```
tsrc IPv4-source-address tdst IPv4-destination-address up
```

b. **(Optional) Add a logical interface for the source IPv6 address and the destination IPv6 addresses.**

```
addif IPv6-source-address IPv6-destination-address
```

Omit this substep if you want the address autoconfigured for this interface. You do not need to configure link-local addresses for your tunnel.

3. **Reboot the system.**

4. **Repeat this task on the opposite endpoint of the tunnel.**

Example 6–2 Entry in the `/etc/hostname6.ip.tun` File for a Manual, IPv6 Over IPv4 Tunnel

This sample `/etc/hostname6.ip.tun` file shows a tunnel for which global source addresses and global destination addresses are manually configured.

```
tsrc 192.168.8.20 tdst 192.168.7.19 up
addif 2001:db8:3c4d:8::fe12:528 2001:db8:3c4d:7:a00:20ff:fe12:1234
```

▼ How to Manually Configure IPv6 Over IPv6 Tunnels

This procedure describes how to set up a tunnel from an IPv6 node to a remote IPv6 node over an IPv6 network.

Steps 1. **Log in to the local tunnel endpoint as Primary Administrator or as superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Create the `/etc/hostname6.ip6.tun n` file.**

Use the values 0, 1, 2, and so on, for *n*. Then, add entries by following these substeps.

a. Add the tunnel source address and the tunnel destination address.

```
tsrc IPv6-source-address tdst IPv6-destination-address  
IPv6-packet-source-address IPv6-packet-destination-address up
```

b. (Optional) Add a logical interface for the source IPv6 address and destination IPv6 address.

```
addif IPv6-source-address IPv6-destination-address up
```

Omit this step if you want the address autoconfigured for this interface. You do not need to configure link-local addresses for your tunnel.

3. Reboot the system.

4. Repeat this procedure at the opposite endpoint of the tunnel.

Example 6–3 Entry in the `/etc/hostname6.ip6.tun` File for an IPv6 Over IPv6 Tunnel

This example shows the entry for an IPv6 over IPv6 tunnel.

```
tsrc 2001:db8:3c4d:22:20ff:0:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3  
fe80::4 fe80::61 up
```

▼ How to Configure IPv4 Over IPv6 Tunnels

This procedure explains how to configure a tunnel between two IPv4 hosts over an IPv6 network. You would use this procedure if your corporate network is heterogeneous, with IPv6 subnets that separate IPv4 subnets.

Steps **1. Log in to the local IPv4 tunnel endpoint as Primary Administrator or as superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Create the `/etc/hostname.ip6.tunn` file.

Use the values 0, 1, 2, and so on, for *n*. Then, add entries by following these steps:

a. Add the tunnel source address and the tunnel destination address.

```
tsrc IPv6-source-address tdst IPv6-destination-address
```

- b. (Optional) Add a logical interface for the source IPv6 address and destination IPv6 address.

```
addif IPv6-source-address IPv6-destination-address up
```

3. Reboot the local host.
4. Repeat this procedure at the opposite endpoint of the tunnel.

Example 6–4 Entry in the `/etc/hostname6.ip6.tun` for an IPv4 Over IPv6 Tunnel

This example shows the entry for an IPv4 over IPv6 tunnel.

```
tsrc 2001:db8:3c4d:114:a00:20ff:fe72:668c tdst 2001:db8:3c4d:103:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

▼ How to Configure a 6to4 Tunnel

If your IPv6 network needs to communicate with a remote IPv6 network, consider using automatic, 6to4 tunnels. The process of configuring a 6to4 tunnel includes configuring the boundary router as a 6to4 router. The 6to4 router functions as the endpoint of a 6to4 tunnel between your network and an endpoint router at a remote IPv6 network.

Before You Begin Before you configure 6to4 routing on an IPv6 network, you must have done the following:

- Configured IPv6 on all appropriate nodes at the prospective 6to4 site, as described in “Configuring IPv6 on a Host” on page 142.
- Selected at least one router with a connection to an IPv4 network to become the 6to4 router.
- Configured a globally unique IPv4 address for the prospective 6to4 router’s interface to the IPv4 network. The IPv4 address must be static.

Note – Do not use a dynamically allocated IPv4 address, as described in [Chapter 11](#). Global dynamically allocated addresses might change over time, which can adversely affect your IPv6 addressing plan.

- Steps**
1. **Log in to the prospective 6to4 router as Primary Administrator or as superuser.**
The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Configure a 6to4 pseudo-interface on the router by creating the /etc/hostname6.ip.6to4tun0 file.**

- If you plan to use the recommended convention of subnet ID=0 and host ID=1, use the short format for /etc/hostname6.ip.6to4tun0:

```
tsrc IPv4-address up
```

- If you plan to use other conventions for the subnet ID and host ID, use the long format for /etc/hostname6.ip.6to4tun0:

```
tsrc IPv4-address 2002:IPv4-address:subnet-ID:interface-ID:/64 up
```

The required parameters for /etc/hostname6.ip.6to4tun0 follow:

<i>tsrc</i>	Indicates that this interface is used as a tunnel source.
<i>IPv4-address</i>	Specifies, in dotted-decimal format, the IPv4 address that is configured on the physical interface to become the 6to4 pseudo-interface.

The remaining parameters are optional. However, if you specify one optional parameter, you must specify all optional parameters.

<i>2002</i>	Specifies the 6to4 prefix.
<i>IPv4-address</i>	Specifies, in hexadecimal notation, the IPv4 address of the pseudo-interface.
<i>subnet-ID</i>	Specifies, in hexadecimal notation, a subnet ID other than 0.
<i>interface-ID</i>	Specifies an interface ID other than 1.
<i>/64</i>	Indicates that the 6to4 prefix has a length of 64 bits.
<i>up</i>	Configures the 6to4 interface as "up."

Note – Two IPv6 tunnels on your network cannot have the same source address and the same destination address. Packets are dropped as a result. This type of event can happen if a 6to4 router also performs tunneling through the `atun` command. For information about `atun`, refer to the `tun(7M)` man page.

3. **(Optional) Create additional 6to4 pseudo-interfaces on the router.**

Each prospective 6to4 pseudo-interface must have an already configured, globally unique IPv4 address.

4. **Reboot the 6to4 router.**

5. **Verify the status of the interface.**

```
# ifconfig ip.6to4tun0 inet6
```

If the interface is correctly configured, you receive output that is similar to the following:

```
ip.6to4tun0: flags=2200041<UP,RUNNING,NOUD,IPv6>mtu 1480 index 11
    inet tunnel src 111.222.33.44
    tunnel hop limit 60
    inet6 2002:6fde:212c:10:/64
```

6. Edit the `/etc/inet/ndpd.conf` file to advertise 6to4 routing.

For detailed information, refer to the `ndpd.conf(4)` man page.

a. Specify the subnet to receive the advertisement in the first line.

Create an `if` entry with the following format:

```
if subnet-interface AdvSendAdvertisements 1
```

For example, to advertise 6to4 routing to the subnet that is connected to interface `hme0`, replace `subnet-interface` with `hme0`.

```
if hme0 AdvSendAdvertisements 1
```

b. Add the 6to4 prefix as the second line of the advertisement.

Create a `prefix` entry with following format:

```
prefix 2002:IPv4-address:subnet-ID::/64 subnet-interface
```

7. Reboot the router.

Alternatively, you can issue a `sigup` to the `/etc/inet/in.ndpd` daemon to begin sending router advertisements. The IPv6 nodes on each subnet to receive the 6to4 prefix now autoconfigure with new 6to4-derived addresses.

8. Add the new 6to4-derived addresses of the nodes to the name service that is used at the 6to4 site.

For instructions, go to “[Configuring Name Service Support for IPv6](#)” on page 138.

Example 6–5 6to4 Router Configuration (Short Form)

The following is an example of the short form of `/etc/hostname6.ip.6to4tun0`:

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 up
```

Example 6–6 6to4 Router Configuration (Long Form)

Here is an example of the long form of `/etc/hostname6.ip.6to4tun0`:

```
# cat /etc/hostname6.ip.6to4tun0
tsrc 111.222.33.44 2002:6fde:212c:20:1/64 up
```

Example 6-7 `ifconfig` Output Showing 6to4 Pseudo-Interface

The following sample shows output of the `ifconfig` command for a 6to4 pseudo-interface:

```
# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NUD,IPv6> mtu 1480 index 11
    inet tunnel src 192.168.87.188
    tunnel hop limit 60
    inet6 2002:c0a8:57bc::1/64
```

Example 6-8 6to4 Advertisements in `/etc/inet/ndpd.conf`

The following sample `/etc/inet/ndpd.conf` file advertises 6to4 routing on two subnets:

```
if qfe0 AdvSendAdvertisements 1
prefix 2002:c0a8:57bc:10::/64 qfe0

if qfe1 AdvSendAdvertisements 1
prefix 2002:c0a8:57bc:2::/64 qfe1
```

More Information

Configuring Multiple Routers at the 6to4 Site

For a multiple router site, the routers behind the 6to4 router might require further configuration to support 6to4. If your site uses RIP, you must configure on each non-6to4 router the static routes to the 6to4 router. If you use a commercial routing protocol, you do not need to create static routes to the 6to4 router.

▼ How to Configure a 6to4 Tunnel to a 6to4 Relay Router



Caution – Because of major security issues, by default, 6to4 relay router support is disabled in the Solaris OS. See [“Security Issues When Tunneling to a 6to4 Relay Router”](#) on page 180.

Before You Begin

Before you enable a tunnel to a 6to4 relay router, you must have completed the following tasks:

- Configured a 6to4 router at your site, as explained in [“How to Configure a 6to4 Tunnel”](#) on page 133
- Reviewed the security issues that are involved in tunneling to a 6to4 relay router

Steps 1. **Log in to the 6to4 router as Primary Administrator or as superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Enable a tunnel to the 6to4 relay router by using either of the following formats:**

- Enable a tunnel to an anycast 6to4 relay router.

```
# /usr/sbin/6to4relay -e
```

The `-e` option sets up a tunnel between the 6to4 router and an anycast 6to4 relay router. Anycast 6to4 relay routers have the well-known IPv4 address 192.88.99.1. The anycast relay router that is physically nearest to your site becomes the endpoint for the 6to4 tunnel. This relay router then handles packet forwarding between your 6to4 site and a native IPv6 site.

For detailed information about anycast 6to4 relay routers, refer to RFC 3068, “An Anycast Prefix for 6to4 Relay Routers” (<ftp://ftp.rfc-editor.org/in-notes/rfc3068.txt>).

- Enable a tunnel to a specific 6to4 relay router.

```
# /usr/sbin/6to4relay -e -a relay-router-address
```

The `-a` option indicates that a specific router address is to follow. Replace *relay-router-address* with the IPv4 address of the specific 6to4 relay router with which you want to enable a tunnel.

The tunnel to the 6to4 relay router remains active until you remove the 6to4 tunnel pseudo-interface.

3. **Delete the tunnel to the 6to4 relay router, when the tunnel is no longer needed:**

```
# /usr/sbin/6to4relay -d
```

4. **(Optional) Make the tunnel to the 6to4 relay router persistent across reboots.**

Your site might have a compelling reason to have the tunnel to the 6to4 relay router reinstated each time the 6to4 router reboots. To support this scenario, you must do the following:

- a. **Edit the `/etc/default/inetinit` file.**

The line that you need to modify is at the end of the file.

- b. **Change the “NO” value in the line `ACCEPT6TO4RELAY=NO` to “YES.”**

- c. **(Optional) Create a tunnel to a specific 6to4 relay router that persists across reboots.**

For the parameter `RELAY6TO4ADDR`, change the address 192.88.99.1 to the IPv4 address of the 6to4 relay router that you want to use.

Example 6–9 Getting Status Information About 6to4 Relay Router Support

You can use the `/usr/bin/6to4relay` command to find out whether support for 6to4 relay routers is enabled. The next example shows the output when support for 6to4 relay routers is disabled, as is the default in the Solaris OS:

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is disabled.
```

When support for 6to4 relay routers is enabled, you receive the following output:

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is enabled.
IPv4 destination address of Relay Router=192.88.99.1
```

Configuring Name Service Support for IPv6

This section describes how to configure the DNS and NIS name services to support IPv6 services.

Note – LDAP supports IPv6 without requiring IPv6-specific configuration tasks.

For full details for administering DNS, NIS, and LDAP, refer to the *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

▼ How to Add IPv6 Addresses to DNS

- Steps**
1. **Log in to the primary or secondary DNS server as Primary Administrator or as superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Edit the appropriate DNS zone file by adding AAAA records for each IPv6-enabled node:**

```
host-name IN AAAA host-address
```

3. Edit the DNS reverse zone file and add PTR records:

```
host-address IN PTR hostname
```

For detailed information on DNS administration, refer to *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Example 6–10 DNS Reverse Zone File

This example shows an IPv6 address in the reverse zone file.

```
$ORIGIN ip6.int.  
8.2.5.0.2.1.e.f.f.f.9.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.2.0.0.0 \  
IN PTR vallejo.Eng.apex.COM.
```

Adding IPv6 Addresses to NIS

Two new maps have been added for NIS: `ipnodes.byname` and `ipnodes.byaddr`. These maps contain both IPv4 and IPv6 host name and address associations. The `hosts.byname` and `hosts.byaddr` maps contain only IPv4 host name and address associations. These maps are unchanged so that they can facilitate existing applications. Administration of the new maps is similar to the administration of the `hosts.byname` and `hosts.byaddr` maps. Again, it is important that when you update the `hosts` maps with IPv4 addresses that the new `ipnode` maps are also updated with the same information.

For instructions on administering NIS maps, refer to Chapter 5, “Setting Up and Configuring NIS Service,” in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Note – Tools that are aware of IPv6 use the new NIS maps.

▼ How to Display IPv6 Name Service Information

You can use the `nslookup` command to display IPv6 name service information.

Steps 1. Under your user account, run the `nslookup` command.

```
% /usr/sbin/nslookup
```

The default server name and address appear, followed by the `nslookup` command’s angle bracket prompt.

2. View information about a particular host by typing the following commands at the angle bracket prompt:

```
>set q=any  
>host-name
```

3. Type the following command to view only AAAA records:

```
>set q=AAAA  
hostname
```

4. Quit the `nslookup` command by typing `exit`.

Example 6–11 Using `nslookup` to Display IPv6 Information

This example shows the results of `nslookup` in an IPv6 network environment.

```
% /usr/sbin/nslookup  
Default Server: dnsserve.local.com  
Address: 10.10.50.85  
> set q=AAAA  
> host85  
Server: dnsserve.local.com  
Address: 10.10.50.85  
  
host85.local.com IPv6 address = 2::9256:a00:fe12:528  
> exit
```

▼ How to Verify That DNS IPv6 PTR Records Are Updated Correctly

In this procedure, you use the `nslookup` command to display PTR records for DNS IPv6.

- Steps**
1. Under your user account, run the `nslookup` command.

```
% /usr/sbin/nslookup
```

The default server name and address display, followed by the `nslookup` command's angle bracket prompt.

2. Type the following at the angle bracket prompt to see the PTR records:

```
>set q=PTR
```

3. Quit the command by typing `exit`.

Example 6–12 Using nslookup to Display PTR Records

The following example shows the PTR record display from the nslookup command.

```
% /usr/sbin/nslookup
Default Server: space1999.Eng.apex.COM
Address: 192.168.15.78
> set q=PTR
> 8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0.ip6.int

8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.0.0.2.0.0.0.ip6.int name =
vallejo.ipv6.Eng.apex.COM
ip6.int nameserver = space1999.Eng.apex.COM
> exit
```

▼ How to Display IPv6 Information Through NIS

In this procedure, you use the `ypmatch` command to display IPv6 information through NIS:

- Step** ● Under your user account, type the following to display IPv6 addresses in NIS:

```
% ypmatch hostname ipnodes.byname
```

The information about the specified *hostname* displays.

Example 6–13 IPv6 Addresses Output by the ypmatch Command

The following sample shows the results of a `ypmatch` operation on the `ipnodes.byname` database.

```
% ypmatch farhost ipnodes.byname
2001:0db8:3c4d:15:a00:20ff:fe12:5286 farhost
```

▼ How to Display IPv6 Information Independent of the Name Service

- Step** ● Under your user account, type the following command:

```
% getent ipnodes hostname
```

The information about the specified *host-name* is displayed.

Example 6–14 Displaying IPv6 Information in the ipnodes Database

The following sample shows the output of the `getent` command:

```
% getent ipnodes vallejo
2001:0db8:8512:2:56:a00:fe87:9aba    myhost myhost
fe80::56:a00:fe87:9aba            myhost myhost
```

Configuring IPv6 on a Host

This section explains how to configure IPv6 on a host. In most instances, you should allow the host to use address autoconfiguration, as explained in [“Stateless Autoconfiguration Overview” on page 82](#). However, if a particular host has an interface that must not be automatically configured, you can use either of two options. You can manually configure the interface ID, as described in [“How to Manually Configure a Link-Local Address” on page 147](#). Alternatively, you can define a temporary address, as explained in [“Using Temporary Addresses for an Interface” on page 144](#).

▼ How to Enable IPv6 Address Autoconfiguration

Before You Begin Before you set up address autoconfiguration on an IPv6 node, you must complete the following tasks.

Task	For Information
Installed the Solaris OS with IPv6 enabled on each node to have autoconfigured IPv6 addresses.	Refer to the installation documentation appropriate to the particular node.
Configured a IPv6 site prefix on a router on the same link as the node to receive the autoconfigured IPv6 address.	“How to Configure an IPv6–Enabled Router” on page 126

Steps 1. **Log in to the new IPv6 host as Primary Administrator or as superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, [“Working With the Solaris Management Console \(Tasks\),”](#) in *System Administration Guide: Basic Administration*.

2. Display the status of the host's interfaces after installation.

```
# ifconfig -a
```

The resulting output shows the interface that was configured for IPv6. In this example, the interface is shown in bold.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
qfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500
    index 2
    inet 172.16.27.74 netmask ffffffff broadcast 172.16.27.255
    ether 0:3:ba:13:14:e1
qfe1: flags=1000862 <BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4>
    mtu 1500 index 3
    inet 0.0.0.0 netmask 0 broadcast 255.255.255.255
    ether 0:3:ba:13:14:e2
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:13:14:e1
    inet6 fe80::203:baff:fe13:14e1/10
```

After the Solaris release is installed with IPv6 enabled, the lowest numbered interface is configured with an IPv6 address. In the previous example, the `qfe0` interface has an automatically configured link-local address.

3. (Optional) Type the following to create IPv6 addresses for any additional interfaces on the host that were not configured during installation.

```
# touch /etc/hostname6.interface
```

4. (Optional) Create an `/etc/inet/ndpd.conf` file that defines parameters for interface variables on the IPv6 host.

If you need to create temporary addresses for the host's interface, refer to ["Using Temporary Addresses for an Interface" on page 144](#). For details about `/etc/inet/ndpd.conf`, refer to the `ndpd.conf(4)man` page and ["ndpd.conf Configuration File" on page 211](#).

5. Reboot the host.

The reboot process sends router discovery packets. The router responds with the site prefix. The response enables the IPv6 host to configure its interfaces with global IPv6 addresses. Rebooting also restarts key network daemons in IPv6 mode.

6. Display the IPv6 addresses of all interfaces.

```
# ifconfig -a6
```

The following example output shows only the IPv6 addresses that are configured on the host's interfaces.

```
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:13:14:e1
    inet6 fe80::203:baff:fe13:14e1/10
qfe0:1: flags=2180841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500
```

7. Repeat Steps 1–6 for all hosts that must be configured with IPv6 addresses.

Using Temporary Addresses for an Interface

You use temporary addresses for any interfaces on a host that you want to keep anonymous. For example, you might want to use temporary addresses for the interfaces of a host that needs to access public web servers. Temporary addresses implement IPv6 privacy enhancements, as described in RFC 3041, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" (<http://www.ietf.org/rfc/rfc3041.txt?number=3041>).

Temporary addresses are autoconfigured by the host. You enable a temporary address in the `/etc/inet/ndpd.conf` file for one or more interfaces, if needed. However, unlike standard, autoconfigured IPv6 addresses, a temporary address consists of the 64-bit subnet prefix and a randomly generated 64-bit number. This random number becomes the interface ID segment of the IPv6 address. A link-local address is not generated with the temporary address as the interface ID.

Be aware that temporary addresses have a default *preferred lifetime* of one day. When you enable temporary address creation, you should also configure the following variables in the `/etc/inet/ndpd.conf` file.

<i>valid lifetime</i>	Time span in which the temporary address exists, after which the address is deleted from the host.
<i>preferred lifetime</i>	Elapsed time before the temporary address is deprecated. This time span should be shorter than the valid lifetime.
<i>address regeneration</i>	Duration of time before the expiration of the preferred lifetime, during which the host should generate a new temporary address.

You express the duration of time for temporary addresses as follows:

<i>n seconds</i>	<i>n</i> number of seconds, which is the default
<i>nh</i>	number of hours (h)
<i>n d</i>	<i>n</i> number of days (d)

▼ How to Configure a Temporary Address

- Steps** 1. Log in to the IPv6 host as Primary Administrator or as superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Enable autoconfigured IP addresses for the host’s interfaces

For autoconfiguration tasks, refer to “How to Enable IPv6 Address Autoconfiguration” on page 142.

3. Edit the `/etc/inet/ndpd.conf` file to turn on temporary address generation.

- To configure temporary addresses on all interfaces of a host, add the following to `/etc/inet/ndpd.conf`:

```
ifdefault TmpAddrsEnabled true
```

- To configure a temporary address for a specific interface, add the following to `/etc/inet/ndpd.conf`:

```
if interface TmpAddrsEnabled true
```

4. (Optional) Specify the valid lifetime for the temporary address.

```
ifdefault TmpValidLifetime duration
```

This syntax specifies the valid lifetime for all interfaces on a host. The value for *duration* should be in seconds, hours, or days. The default valid lifetime is seven days. You can also use `TmpValidLifetime` with the `if interface` keywords to specify the valid lifetime for a temporary address of a particular interface.

5. Specify a preferred lifetime for the temporary address, after which the address is deprecated.

```
if interface TmpPreferredLifetime duration
```

This syntax specifies the preferred lifetime for the temporary address of a particular interface. The default preferred lifetime is one day. You can also use `TmpPreferredLifetime` with the `ifdefault` keyword to specify the preferred lifetime for the temporary addresses on all interfaces of a host.

Note – Default address selection gives a lower priority to IPv6 addresses that have been deprecated. If an IPv6 temporary address is deprecated, default address selection chooses a non deprecated address as the source address of a packet. A non deprecated address could be the automatically generated IPv6 address or, possibly, the interface’s IPv4 address. For more information on default address selection, see “Administering Default Address Selection” on page 173.

6. Specify the lead time in advance of address deprecation, during which the host should generate a new temporary address.

```
ifdefault TmpRegenAdvance duration
```

This syntax specifies the lead time in advance of address deprecation for the temporary addresses of all interfaces on a host. The default is five seconds.

7. Change the configuration of the `in.ndpd` daemon.

```
# pkill in.ndpd
# /usr/lib/inet/in.ndpd
```

8. Verify that temporary addresses have been created by running the `ifconfig -a` command.

The output from `ifconfig` should have the word `TEMPORARY` in the same line as the interface definition, as shown in [Example 6-16](#).

Example 6-15 Temporary Address Variables in `/etc/inet/ndpd.conf`

The following example shows a segment of an `/etc/inet/ndpd.conf` file with temporary addresses enabled for the primary network interface.

```
ifdefault TmpAddrsEnabled true

ifdefault TmpValidLifetime 14d

ifdefault TmpPreferredLifetime 7d

ifdefault TmpRegenAdvance 6s
```

Example 6-16 `ifconfig` Output with Temporary Addresses Enabled

This example shows the output of the `ifconfig` command after temporary addresses are created.

```
# ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.112 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:b9:4c:54
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
hme0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 8:0:20:b9:4c:54
    inet6 fe80::a00:20ff:feb9:4c54/10
hme0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
    inet6 2001:db8:3c4d:15:a00:20ff:feb9:4c54/64
hme0:2: flags=802080841<UP,RUNNING,MULTICAST,ADDRCONF,IPv6,TEMPORARY> mtu 1500 index 2
    inet6 2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64
```

Note that the line following interface `hme0:2` includes the word `TEMPORARY`. This designation indicates that the address `2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64` has a temporary interface ID.

- See Also**
- To set up name service support for IPv6 addresses, see [“Configuring Name Service Support for IPv6” on page 138](#).
 - To configure IPv6 addresses for a server, see [“How to Manually Configure a Link-Local Address” on page 147](#).
 - To monitor activities on IPv6 nodes, see [Chapter 7](#).

Configuring IPv6 on Servers

To avoid erroneous IPv6 addresses that result from replacing NIC cards, you should manually configure the interfaces of an IPv6 server. Do not use autoconfigured IPv6 addresses. Instead, define the server’s IPv6 addresses by using a link-local address that contains a *token*. When you configure a token for an interface, Neighbor Discovery does not create a link-local address that is based on the interface’s MAC address. Instead, the manually created token becomes the interface ID in the link-local address. To create the token, you specify a hexadecimal number of 64 bits or less to occupy the interface ID portion of the IPv6 address. This token remains assigned to the interface, even when a card is replaced.

▼ How to Manually Configure a Link-Local Address

Note – Although the following instructions are written specifically for servers, they also are valid for configuring manual link-local addresses on any IPv6 node.

Before You Begin

You must do the following before configuring IPv6 on the server.

Task	For Information
1. If applicable, upgrade the application software to support IPv6. Note that many applications that run on the IPv4 protocol stack also successfully run on IPv6.	“How to Prepare Network Services for IPv6 Support” on page 90

Task	For Information
2. Create one or more 64-bit hexadecimal addresses as the link-local addresses for the interfaces of the server.	“Link-Local Unicast Address” on page 79
3. Install the Solaris OS with IPv6-enabled on the server.	<i>Solaris 10 Installation Guide: Basic Installations</i>

Steps 1. **On the server, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Check the status of the server’s interfaces.**

```
# ifconfig -a
```

The following output shows that the interface that is shown in bold type has an IPv6 address.

```
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
dmfe0: flags=1000863 <UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 172.16.15.74 netmask ffffffff broadcast 172.16.27.255
    ether 0:3:ba:13:14:e1
dmfe1: flags=1000862 <BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 0.0.0.0 netmask 0 broadcast 255.255.255.255
    ether 0:3:ba:13:14:e2
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
dmfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:13:14:e1
inet6 fe80::203:baff:fe13:14e1/10
```

The preceding output shows that the primary network interface, `dmfe0`, has the link-local address `fe80::203:baff:fe13:14e1/10`. This address was automatically configured during installation. The second interface, `dmfe1`, is not currently configured.

3. **Edit the existing `/etc/hostname6.interface` file or files that were created during installation.**

Note – You do not have to manually configure IPv6 interface IDs on any or all interfaces on a server. However, you should consider this approach if you swap out regularly interface cards.

4. **Configure each interface with a token.**

Use the following form of the `ifconfig` command for each interface that has a manually assigned interface ID.

```
ifconfig interface token address/prefix-length plumb up
```

For example, you use the following command to configure interface `dmfe0` with a token:

```
# ifconfig dmfe0 token fe80::203:baff:fe15:15e1/10 plumb up
```

Repeat this step for every interface with a manually configured interface ID.

5. Create an `/etc/inet/ndpd.conf` file that defines interface variables for the particular server.

`/etc/inet/ndpd.conf` should have the following contents in order to turn off address autoconfiguration for all of the server's interfaces.

```
if-variable-name StatelessAddrConf false
```

Refer to `thendpd.conf(4)` man page and "[ndpd.conf Configuration File](#)" on page 211 for more information.

6. Turn off routing and IP forwarding on all of the server's interfaces.

```
# routeadm -d ipv6-routing ipv6-forwarding
# routeadm -d
# routeadm -u
```

7. Update the IPv6 daemon with your changes.

```
# pkill -HUP -in.ndpd
```

- See Also**
- To update the name services with the IPv6 addresses of the server, see "[Configuring Name Service Support for IPv6](#)" on page 138.
 - To monitor server performance, see [Chapter 7](#).

Administering a TCP/IP Network (Tasks)

This chapter contains tasks for administering a TCP/IP network. The following topics are covered:

- “Major TCP/IP Administrative Tasks (Task Map)” on page 152
- “Monitoring the Interface Configuration With the `ifconfig` Command” on page 153
- “Monitoring Network Status With the `netstat` Command” on page 157
- “Probing Remote Hosts With the `ping` Command” on page 164
- “Administering and Logging Network Status Displays” on page 165
- “Displaying Routing Information With the `traceroute` Command” on page 168
- “Monitoring Packet Transfers With the `snoop` Command” on page 170
- “Administering Default Address Selection” on page 173

The tasks assume that you have an operational TCP/IP network at your site, either IPv4-only or dual-stack IPv4/IPv6. If you want to implement IPv6 at your site but have not done so, refer to following chapters for more information:

- To plan an IPv6 implementation, refer to [Chapter 4](#).
- To configure IPv6 and create a dual-stack network environment, refer to [Chapter 6](#).

Major TCP/IP Administrative Tasks (Task Map)

Task	Description	For Information
Display configuration information about an interface.	Determine the current configuration of each interface on a system.	"How to Get Information About a Specific Interface" on page 153
Display interface address assignments.	Determine the address assignments for all interfaces on the local system.	"How to Display Interface Address Assignments" on page 155
Display statistics on a per-protocol basis.	Monitor the performance of the network protocols on a particular system.	"How to Display Statistics by Protocol" on page 157
Display network status.	Monitor your system by displaying all sockets and routing table entries. The output includes the inet address family for IPv4 and inet6 address family for IPv6.	"How to Display the Status of Sockets" on page 160
Display the status of network interfaces.	Monitor the performance of network interfaces, which is useful for troubleshooting transmission problems.	"How to Display Network Interface Status" on page 160
Display packet transmission status.	Monitor the state of packets as they are sent over the wire.	"How to Display the Status of Transmissions for Packets of a Specific Address Type" on page 162
Control the display output of IPv6-related commands.	Controls the output of the ping, netstat, ifconfig, and traceroute commands. Creates a file that is named inet_type. Sets the DEFAULT_IP variable in this file.	"How to Control the Display Output of IP-Related Commands" on page 165
Monitor network traffic.	Displays all IP packets by using the snoop command.	"How to Monitor IPv6 Network Traffic" on page 173
Trace all routes that are known to the network's routers.	Uses the traceroute command to show all routes.	"How to Trace All Routes" on page 169

Monitoring the Interface Configuration With the `ifconfig` Command

You use the `ifconfig` command to manually assign IP addresses to interfaces and to manually configure interface parameters. In addition, the Solaris startup scripts run `ifconfig` to configure pseudo interfaces, such as 6to4 tunnel endpoints.

This book contains many tasks that use the various options of the versatile `ifconfig` command. For a complete description of this command, its options, and its variables, refer to the `ifconfig(1M)` man page. The basic syntax of `ifconfig` follows:

```
ifconfig interface [protocol-family]
```

▼ How to Get Information About a Specific Interface

Use the `ifconfig` command to determine basic information about the interfaces of a particular system. For example, a simple `ifconfig` query can tell you the following:

- Device names of all interfaces on a system
- All IPv4 and, if applicable, all IPv6 addresses that are assigned to the interfaces
- Whether these interfaces are currently configured

The following procedure shows how to use the `ifconfig` command to obtain basic configuration information about a system's interfaces.

Steps 1. On the local host, assume the Primary Administrator role, or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, "Working With the Solaris Management Console (Tasks)," in *System Administration Guide: Basic Administration*.

2. Obtain information about a particular interface.

```
# ifconfig interface
```

The output from the `ifconfig` command has the following format:

- Status line

The first line in the `ifconfig` command output includes the interface name and status flags currently associated with the interface. Also, the status line includes the maximum transmission unit (MTU) that is configured for the particular interface and an index number. Use the status line to determine the current state of the interface.

- IP address information line

The second line of the `ifconfig` output includes the IPv4 address or IPv6 address that is configured for the interface. For an IPv4 address, the configured netmask and broadcast address are also displayed.

- MAC address line

When you run the `ifconfig` command as superuser or with a similar role, the `ifconfig` output contains a third line. For an IPv4 address, the third line shows the MAC address (Ethernet layer address) that is assigned to the interface. For an IPv6 address, the third line in the output shows the link-local address that the IPv6 `in.ndpd` daemon generates from the MAC address.

Example 7-1 Basic Interface Information From the `ifconfig` Command

The following example shows how to obtain information about the `eri` interface on a particular host by using the `ifconfig` command.

```
# ifconfig eri
eri0: flags=863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 1
      inet 10.0.0.112 netmask ffffffff broadcast 10.8.48.127
      ether 8:0:20:b9:4c:54
```

The next table describes the variable information in an `ifconfig` query. The preceding output is used as an example.

Variable	Screen Output	Description
Interface name	<code>eri0</code>	Indicates the device name of the interface whose status was requested in the <code>ifconfig</code> command.
Interface status	<code>flags=863<UP</code>	Displays the status of the interface, including any flags that are currently associated with the interface. Here you can determine whether the interface is currently initialized (<code>UP</code>) or not initialized (<code>DOWN</code>).
Broadcast status	<code>BROADCAST</code>	Indicates that the interface supports IPv4 broadcasts.
Transmission status	<code>RUNNING</code>	Indicates that the system is transmitting packets through the interface.
Multicast status	<code>MULTICAST, IPv4</code>	Shows that the interface supports multicast transmissions. The example interface supports IPv4 multicast transmissions.
Maximum transmission unit	<code>mtu 1500</code>	Shows that this interface has a maximum transfer size of 1500 octets.
IP address	<code>inet 10.0.0.112</code>	Displays the IPv4 or IPv6 address that is assigned to the interface. Example interface <code>eri0</code> has the IPv4 address <code>10.0.0.112</code> .
Netmask	<code>netmask ffffffff80</code>	Displays the IPv4 netmask of the particular interface. Note that IPv6 addresses do not use netmasks.

Variable	Screen Output	Description
MAC address	ether 8:0:20:b9:4c:54	Shows the interface's Ethernet layer address.

▼ How to Display Interface Address Assignments

Routers and multihomed hosts have more than one interface and, often, more than one IP address assigned to each interface. You can use the `ifconfig` command to display all addresses that are assigned to the interfaces of a system. You can also use the `ifconfig` command to display only IPv4 or IPv6 address assignments. To additionally display the MAC addresses of the interfaces, you must first log in as superuser or assume the appropriate role.

For more information on the `ifconfig` command, see the `ifconfig(1M)` man page.

Steps 1. On the local system, assume the Network Management role or become superuser.

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. Obtain information about all interfaces.

You can use variations of the `ifconfig -a` command to do the following:

- View all addresses of all interfaces on the system.
- View all IPv4 addresses that are assigned to a system's interfaces.
- If the local system is IPv6-enabled, display all IPv6 addresses that are assigned to a system's interfaces.

```
ifconfig -a6
```

Example 7–2 Displaying Addressing Information for All Interfaces

This example shows entries for a host with solely a primary network interface, `qfe0`. Nevertheless, the `ifconfig` output shows that three forms of addresses are currently assigned to `qfe0`: loopback (`lo0`), IPv4 (`inet`), and IPv6 (`inet6`). In the IPv6 section of the output, note that the line for interface `qfe0` displays the link-local IPv6 address. The second address for `qfe0` is displayed on the `qfe0:1` line.

```
% ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
```

```

qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.112 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:b9:4c:54
lo0: flags=2000849 <UP,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 8:0:20:b9:4c:54
    inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
    inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64

```

Example 7-3 Displaying Addressing Information for All IPv4 Interfaces

This example shows the IPv4 address that is configured for a multihomed host. You do not need to be logged in as superuser to run this form of the `ifconfig` command.

```

% ifconfig -a4
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
qfe0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.112 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:b9:4c:54
qfe1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.118 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:6f:5e:17

```

Example 7-4 Displaying Addressing Information for All IPv6 Interfaces

This example shows only the IPv6 addresses that are configured for a particular host. You do not need to be logged in as superuser to run this form of the `ifconfig` command.

```

% ifconfig -a6
lo0: flags=2000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
qfe0: flags=2000841 <UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 8:0:20:b9:4c:54
    inet6 fe80::a00:20ff:feb9:4c54/10
qfe0:1: flags=2080841 <UP,RUNNING,MULTICAST,ADDRCONF,IPv6> mtu 1500 index 2
    inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64

```

This output from `ifconfig` shows the following three types of IPv6 address forms that are assigned to the single interface of a host:

```

lo0
    IPv6 loopback address.

inet6 fe80::a00:20ff:feb9:4c54/10
    Link-local address that is assigned to the primary network interface.

inet6 2001:db8:3c4d:48:a00:20ff:feb9:4c54/64
    IPv6 address, including subnet prefix. The term ADDRCONF in the output indicates
    that this address was autoconfigured by the host.

```

Monitoring Network Status With the netstat Command

The `netstat` command generates displays that show network status and protocol statistics. You can display the status of TCP, SCTP, and UDP endpoints in table format. You can also display routing table information and interface information.

The `netstat` command displays various types of network data, depending on the selected command-line option. These displays are the most useful for system administration. The basic syntax for `netstat` follows:

```
netstat [-m] [-n] [-s] [-i | -r] [-faddress-family]
```

This section describes the most commonly used options of the `netstat` command. For a detailed description of all `netstat` options, refer to the `netstat(1M)` man page.

▼ How to Display Statistics by Protocol

The `netstat -s` option displays protocol statistics for the UDP, TCP, SCTP, ICMP, and IP protocols.

Note – You can use your Solaris user account to obtain output from the `netstat` command.

Step ● Display the protocol status.

```
$ netstat -s
```

Example 7-5 Network Protocol Statistics

The following example shows the output of the `netstat -s` command. Parts of the output have been truncated. The output can indicate areas where a protocol is having problems. For example, statistical information from ICMPv4 and ICMPv6 can indicate where the ICMP protocol has found errors.

```
RAWIP
rawipInDatagrams    = 4701    rawipInErrors      = 0
rawipInChecksumErrs = 0       rawipOutDatagrams  = 4
rawipOutErrors      = 0
```

UDP

```

        udpInDatagrams      = 10091      udpInErrors      = 0
        udpOutDatagrams     = 15772      udpOutErrors     = 0

TCP      tcpRtoAlgorithm          = 4          tcpRtoMin        = 400
        tcpRtoMax          = 60000      tcpMaxConn       = -1
        .
        .
        tcpListenDrop     = 0          tcpListenDropQ0 = 0
        tcpHalfOpenDrop   = 0          tcpOutSackRetrans = 0

IPv4     ipForwarding          = 2          ipDefaultTTL     = 255
        ipInReceives      = 300182     ipInHdrErrors    = 0
        ipInAddrErrors    = 0          ipInCksumErrs   = 0
        .
        .
        ipsecInFailed      = 0          ipInIPv6         = 0
        ipOutIPv6         = 3          ipOutSwitchIPv6  = 0

IPv6     ipv6Forwarding   = 2          ipv6DefaultHopLimit = 255
        ipv6InReceives    = 13986     ipv6InHdrErrors  = 0
        ipv6InTooBigErrors = 0          ipv6InNoRoutes   = 0
        .
        .
        rawipInOverflows  = 0          ipv6InIPv4       = 0
        ipv6OutIPv4       = 0          ipv6OutSwitchIPv4 = 0

ICMPv4   icmpInMsgs       = 43593     icmpInErrors     = 0
        icmpInCksumErrs   = 0          icmpInUnknowns   = 0
        .
        .
        icmpInOverflows   = 0

ICMPv6   icmp6InMsgs     = 13612     icmp6InErrors    = 0
        icmp6InDestUnreachs = 0      icmp6InAdminProhibs = 0
        .
        .
        icmp6OutGroupQueries = 0      icmp6OutGroupResps = 2
        icmp6OutGroupReds   = 0

IGMP:
12287 messages received
    0 messages received with too few bytes
    0 messages received with bad checksum
12287 membership queries received
SCTP     sctpRtoAlgorithm   = vanj
        sctpRtoMin        = 1000
        sctpRtoMax        = 60000
        sctpRtoInitial    = 3000
        sctpTimHearBeatProbe = 2
        sctpTimHearBeatDrop = 0
        sctpListenDrop    = 0
        sctpInClosed      = 0

```

▼ How to Display the Status of Transport Protocols

You can display the status of the transport protocols through the `netstat` command. For detailed information, refer to the `netstat(1M)` man page.

Steps 1. Display the status of the TCP and SCTP transport protocols on a system.

```
$ netstat
```

2. Display the status of a particular transport protocol on a system.

```
$ netstat -p transport-protocol
```

Values for the `transport-protocol` variable are `tcp`, `sctp`, or `udp`.

Example 7-6 Displaying the Status of the TCP and SCTP Transport Protocols

This example shows the output of the basic `netstat` command. Note that IPv4-only information is displayed.

```
$ netstat

TCP: IPv4
  Local Address      Remote Address      Swind Send-Q  Rwind Recv-Q  State
-----
lhost-1.login       abc.def.local.Sun.COM.980 49640    0    49640    0 ESTABLISHED
lhost-1.login       ghi.jkl.local.Sun.COM.1020 49640    1    49640    0 ESTABLISHED
remhost-1.1014      mno.pqr.remote.Sun.COM.nfsd 49640    0    49640    0 TIME_WAIT
SCTP:
Local Address      Remote Address      Swind  Send-Q  Rwind  Recv-Q  StrsI/O  State
-----
*.echo             0.0.0.0             0       0 102400    0    128/1    LISTEN
*.discard          0.0.0.0             0       0 102400    0    128/1    LISTEN
*.9001             0.0.0.0             0       0 102400    0    128/1    LISTEN
```

Example 7-7 Displaying the Status of a Particular Transport Protocol

This example shows the results when you specify the `-P` option of `netstat`.

```
$ netstat -P tcp

TCP: IPv4
  Local Address      Remote Address      Swind Send-Q  Rwind Recv-Q  State
-----
lhost-1.login       abc.def.local.Sun.COM.980 49640    0    49640    0 ESTABLISHED
lhost.login         ghi.jkl.local.Sun.COM.1020 49640    1    49640    0 ESTABLISHED
remhost.1014        mno.pqr.remote.Sun.COM.nfsd 49640    0    49640    0 TIME_WAIT

TCP: IPv6
  Local Address      Remote Address      Swind Send-Q  Rwind Recv-Q  State If
-----
localhost.38983     localhost.32777     49152    0 49152    0 ESTABLISHED
localhost.32777     localhost.38983     49152    0 49152    0 ESTABLISHED
```

```
localhost.38986  localhost.38980  49152  0 49152  0 ESTABLISHED
```

▼ How to Display Network Interface Status

The `i` option of the `netstat` command shows the state of the network interfaces that are configured on the local system. With this option, you can determine the number of packets a system transmits and receives on each network.

Step ● **Display the status of interfaces on the network.**

```
$ netstat -i
```

Example 7-8 Network Interface Status Display

The next example shows the status of IPv4 and IPv6 packet flow through the host's interfaces.

For example, the input packet count (`Ipkts`) that is displayed for a server can increase each time a client tries to boot, while the output packet count (`Opkts`) remains steady. This outcome suggests that the server is seeing the boot request packets from the client. However, the server does not know to respond to them. This confusion might be caused by an incorrect address in the `hosts`, `ipnodes`, or `ethers` database.

However, if the input packet count is steady over time, then the machine does not see the packets at all. This outcome suggests a different type of failure, possibly a hardware problem.

```
Name Mtu Net/Dest Address Ipkts Ierrs Opkts Oerrs Collis Queue
lo0 8232 loopback localhost 142 0 142 0 0 0
hme0 1500 host58 host58 1106302 0 52419 0 0 0

Name Mtu Net/Dest Address Ipkts Ierrs Opkts Oerrs Collis
lo0 8252 localhost localhost 142 0 142 0 0
hme0 1500 fe80::a00:20ff:feb9:4c54/10 fe80::a00:20ff:feb9:4c54 1106305 0 52422 0 0
```

▼ How to Display the Status of Sockets

The `-a` option of the `netstat` command enables you to view the status of sockets on the local host.

Step ● **Type the following to display the status of sockets and routing table entries:**

You can use your user account to run this option of `netstat`.

```
% netstat -a
```


Example 7-9 Displaying All Sockets and Routing Table Entries

The output of the `netstat -a` command shows extensive statistics. The following example shows portions of typical `netstat -a` output.

```
UDP: IPv4
  Local Address          Remote Address      State
-----
    *.bootpc              Idle
host85.bootpc           Idle
    *. *                  Unbound
    *. *                  Unbound
    *.sunrpc              Idle
    *. *                  Unbound
    *.32771               Idle
    *.sunrpc              Idle
    *. *                  Unbound
    *.32775               Idle
    *.time                Idle
    .
    .
    *.daytime              Idle
    *.echo                 Idle
    *.discard              Idle

UDP: IPv6
  Local Address          Remote Address      State      If
-----
    *. *                  Unbound
    *. *                  Unbound
    *.sunrpc              Idle
    *. *                  Unbound
    *.32771               Idle
    *.32778               Idle
    *.syslog              Idle
    .
    .

TCP: IPv4
  Local Address          Remote Address      Swind Send-Q Rwind Recv-Q  State
-----
    *. *                  *. *                0      0 49152    0 IDLE
localhost.4999          *. *                0      0 49152    0 LISTEN
    *.sunrpc              *. *                0      0 49152    0 LISTEN
    *. *                  *. *                0      0 49152    0 IDLE
    *.sunrpc              *. *                0      0 49152    0 LISTEN
    .
    .
    *.printer             *. *                0      0 49152    0 LISTEN
    *.time                *. *                0      0 49152    0 LISTEN
    *.daytime             *. *                0      0 49152    0 LISTEN
    *.echo                 *. *                0      0 49152    0 LISTEN
    *.discard             *. *                0      0 49152    0 LISTEN
    *.chargen             *. *                0      0 49152    0 LISTEN
    *.shell                *. *                0      0 49152    0 LISTEN
    *.shell                *. *                0      0 49152    0 LISTEN
```

```

*.kshell          *.*          0      0 49152      0 LISTEN
*.login
.
.
*.               0      0 49152      0 LISTEN
*TCP: IPv6
Local Address      Remote Address      Swind Send-Q Rwind Recv-Q  State If
-----
*.*               *.*               0      0 49152      0      IDLE
*.sunrpc          *.*               0      0 49152      0      LISTEN
*.*               *.*               0      0 49152      0      IDLE
*.32774           *.*               0      0 4915      0

```

▼ How to Display the Status of Transmissions for Packets of a Specific Address Type

Use the `-f` option of the `netstat` command to view statistics related to packet transmissions of a particular address family.

Step ● View statistics for transmissions of either IPv4 or IPv6 packets.

```
$ netstat -f inet | inet6
```

To view IPv4 transmission information, type `inet` as the argument to `netstat -f`. Use `inet6` as the argument to `netstat -f` to view IPv6 information.

Example 7-10 Status of IPv4 Packet Transmission

The following example shows output from the `netstat -f inet` command.

```

TCP: IPv4
Local Address      Remote Address      Swind Send-Q Rwind Recv-Q  State
-----
host58.734         host19.nfsd         49640  0 49640      0 ESTABLISHED
host58.38063       host19.32782        49640  0 49640      0 CLOSE_WAIT
host58.38146       host41.43601        49640  0 49640      0 ESTABLISHED
host58.996         remote-host.login   49640  0 49206      0 ESTABLISHED

```

Example 7-11 Status of IPv6 Packet Transmission

The following example shows output from the `netstat -f inet6` command.

```

TCP: IPv6
Local Address      Remote Address      Swind Send-Q Rwind Recv-Q  State  If
-----
localhost.38065    localhost.32792     49152  0 49152      0 ESTABLISHED
localhost.32792    localhost.38065     49152  0 49152      0 ESTABLISHED
localhost.38089    localhost.38057     49152  0 49152      0 ESTABLISHED

```

▼ How to Display the Status of Known Routes

The `-r` option of the `netstat` command displays the routing table for the local host. This table shows the status of all routes that the host knows about. You can run this option of `netstat` from your user account.

Step ● Display the IP routing table.

```
$ netstat -r
```

Example 7-12 Routing Table Output by the `netstat` Command

The following example shows output from the `netstat -r` command.

Routing Table: IPv4

Destination	Gateway	Flags	Ref	Use	Interface
host15	myhost	U	1	31059	hme0
10.0.0.14	myhost	U	1	0	hme0
default	distantrouter	UG	1	2	hme0
localhost	localhost	UH	42019361		lo0

Routing Table: IPv6

Destination/Mask	Gateway	Flags	Ref	Use	If
2002:0a00:3010:2::/64	2002:0a00:3010:2:1b2b:3c4c:5e6e:abcd	U	1	0	hme0:1
fe80::/10	fe80::1a2b:3c4d:5e6f:12a2	U	1	23	hme0
ff00::/8	fe80::1a2b:3c4d:5e6f:12a2	U	1	0	hme0
default	fe80::1a2b:3c4d:5e6f:12a2	UG	1	0	hme0
localhost	localhost	UH	9	21832	lo0

Parameter	Description
Destination	Specifies the host that is the destination endpoint of the route.
Destination/Mask	Note that the IPv6 routing table shows the prefix for a 6to4 tunnel endpoint (2002:0a00:3010:2::/64) as the route destination endpoint.
Gateway	Specifies the gateway to use for forwarding packets.
Flags	Indicates the current status of the route. The U flag indicates that the route is up. The G flag indicates that the route is to a gateway.
Use	Shows the number of packets sent.
Interface	Indicates the particular interface on the local host that is the source endpoint of the transmission.

Probing Remote Hosts With the ping Command

You can use the `ping` command to determine the status of a remote host. When you run `ping`, the ICMP protocol sends a datagram to the host that you specify, asking for a response. ICMP is the protocol responsible for error handling on a TCP/IP network. When you use `ping`, you can find out whether an IP connection exists for the specified remote host.

The following is the basic syntax of `ping`:

```
/usr/sbin/ping host [timeout]
```

In this syntax, *host* is the name of the remote host. The optional *timeout* argument indicates the time in seconds for the `ping` command to continue trying to reach the remote host. The default is 20 seconds. For additional syntax and options, refer to the `ping(1M)` man page.

▼ How to Determine if a Remote Host Is Running

Step ● Type the following form of the `ping` command:

```
$ ping hostname
```

If host *hostname* is accepting ICMP transmissions, this message is displayed:

```
hostname is alive
```

This message indicates that *hostname* responded to the ICMP request. However, if *hostname* is down or cannot receive the ICMP packets, you receive the following response from the `ping` command:

```
no answer from hostname
```

▼ How to Determine if a Host Is Dropping Packets

Use the `-s` option of the `ping` command to determine if a remote host is running but nevertheless losing packets.

Step ● Type the following form of the `ping` command:

```
$ ping -s hostname
```

Example 7-13 ping Output for Detecting Packet Dropping

The `ping -s hostname` command continually sends packets to the specified host until you send an interrupt character or a timeout occurs. The responses on your screen resemble the following:

```
PING host1.domain8 : 56 data bytes
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=0. time=74. ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=1. time=73. ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=2. time=74. ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=3. time=74. ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=4. time=74. ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=5. time=73. ms
^C
----host1.domain8 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 73/73/75
```

The packet-loss statistic indicates whether the host has dropped packets. If ping fails, check the status of the network that is reported by the `ifconfig` and `netstat` commands. Refer to [“Monitoring the Interface Configuration With the ifconfig Command” on page 153](#) and [“Monitoring Network Status With the netstat Command” on page 157](#).

Administering and Logging Network Status Displays

The following tasks show how to check the status of the network by using well-known networking commands.

▼ How to Control the Display Output of IP-Related Commands

You can control the output of the `netstat` and `ifconfig` commands to display IPv4 information only, or both IPv4 and IPv6 information.

- Steps**
1. Create the `/etc/default/inet_type` file.
 2. Add one of the following entries to `/etc/default/inet_type`, as required for your network:
 - To display IPv4 information only:

```
DEFAULT_IP=IP_VERSION4
```

- To display both IPv4 and IPv6 information:

```
DEFAULT_IP=BOTH
```

Or

```
DEFAULT_IP=IP_VERSION6
```

For more information about the `inet_type` file, see the `inet_type(4)` man page.

Note – The `-4` and `-6` flags in the `ifconfig` command override the values set in the `inet_type` file. The `-f` flag in the `netstat` command also overrides the values set in the `inet_type` file.

Example 7-14 Controlling Output to Select IPv4 and IPv6 Information

- When you specify the `DEFAULT_IP=BOTH` or `DEFAULT_IP=IP_VERSION6` variable in the `inet_type` file, you should have the following output:

```
% ifconfig -a
lo0: flags=1000849 mtu 8232 index 1
      inet 10.10.0.1 netmask ff000000
qfe0: flags=1000843 mtu 1500 index 2
      inet 10.46.86.54 netmask ffffffff00 broadcast 10.46.86.255
      ether 8:0:20:56:a8
lo0: flags=2000849 mtu 8252 index 1
      inet6 ::1/128
qfe0: flags=2000841 mtu 1500 index 2
      ether 8:0:20:56:a8
      inet6 fe80::a00:fe73:56a8/10
qfe0:1: flags=2080841 mtu 1500 index 2
      inet6 2001:db8:3c4d:5:a00:fe73:56a8/64
```

- When you specify the `DEFAULT_IP=IP_VERSION4` or `DEFAULT_IP=IP_VERSION6` variable in the `inet_type` file, you should have the following output:

```
% ifconfig -a
lo0: flags=849 mtu 8232
      inet 10.10.0.1 netmask ff000000
qfe0: flags=843 mtu 1500
      inet 10.46.86.54 netmask ffffffff00 broadcast 10.46.86.255
      ether 8:0:20:56:a8
```

▼ How to Log Actions of the IPv4 Routing Daemon

If you suspect a malfunction of `routed`, the IPv4 routing daemon, you can start a log that traces the daemon's activity. The log includes all packet transfers when you start the `routed` daemon.

- Steps** 1. **On the local host, assume the Primary Administrator role, or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Create a log file of routing daemon actions:**

```
# /usr/sbin/in.routed /var/log-file-name
```



Caution – On a busy network, this command can generate almost continuous output.

Example 7–15 Network Log for the `in.routed` Daemon

The following example shows the beginning of the log that is created by the procedure “How to Log Actions of the IPv4 Routing Daemon” on page 166.

```
-- 2003/11/18 16:47:00.000000 --
Tracing actions started
RCVBUF=61440
Add interface lo0 #1 127.0.0.1 -->127.0.0.1/32
  <UP|LOOPBACK|RUNNING|MULTICAST|IPv4> <PASSIVE>
Add interface hme0 #2 10.10.48.112 -->10.10.48.0/25
  <UP|BROADCAST|RUNNING|MULTICAST|IPv4>
turn on RIP
Add 10.0.0.0 -->10.10.48.112 metric=0 hme0 <NET_SYN>
Add 10.10.48.85/25 -->10.10.48.112 metric=0 hme0 <IF|NOPROP>
```

▼ How to Trace the Activities of the IPv6 Neighbor Discovery Daemon

If you suspect a malfunction of the IPv6 `in.ndpd` daemon, you can start a log that traces the daemon’s activity. This trace is displayed on the standard output until terminated. This trace includes all packet transfers when you start the `in.ndpd` daemon.

- Steps** 1. **Assume the Primary Administrator role, or become superuser, on the local IPv6 node.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Start a trace of the `in.ndpd` daemon.**

```
# /usr/lib/inet/in.ndpd -t
```

3. Terminate the trace as needed by typing Control-C.

Example 7-16 Trace of the `in.ndpd` Daemon

The following output shows the beginning of a trace of `in.ndpd`.

```
# /usr/lib/inet/in.ndpd -t
Nov 18 17:27:28 Sending solicitation to ff02::2 (16 bytes) on hme0
Nov 18 17:27:28     Source LLA: len 6 <08:00:20:b9:4c:54>
Nov 18 17:27:28 Received valid advert from fe80::a00:20ff:fee9:2d27 (88 bytes) on hme0
Nov 18 17:27:28     Max hop limit: 0
Nov 18 17:27:28     Managed address configuration: Not set
Nov 18 17:27:28     Other configuration flag: Not set
Nov 18 17:27:28     Router lifetime: 1800
Nov 18 17:27:28     Reachable timer: 0
Nov 18 17:27:28     Reachable retrans timer: 0
Nov 18 17:27:28     Source LLA: len 6 <08:00:20:e9:2d:27>
Nov 18 17:27:28     Prefix: 2001:08db:3c4d:1::/64
Nov 18 17:27:28         On link flag:Set
Nov 18 17:27:28         Auto addrconf flag:Set
Nov 18 17:27:28         Valid time: 2592000
Nov 18 17:27:28         Preferred time: 604800
Nov 18 17:27:28     Prefix: 2002:0a00:3010:2::/64
Nov 18 17:27:28         On link flag:Set
Nov 18 17:27:28         Auto addrconf flag:Set
Nov 18 17:27:28         Valid time: 2592000
Nov 18 17:27:28         Preferred time: 604800
```

Displaying Routing Information With the `traceroute` Command

The `traceroute` command traces the route an IP packet follows to a remote system. For technical details about `traceroute`, see the `traceroute(1M)` man page.

You use the `traceroute` command to uncover any routing misconfiguration and routing path failures. If a particular host is unreachable, you can use `traceroute` to see what path the packet follows to the remote host and where possible failures might occur.

The `traceroute` command also displays the round trip time for each gateway along the path to the target host. This information can be useful for analyzing where traffic is slow between the two hosts.

▼ How to Find Out the Route to a Remote Host

Step ● Type the following to discover the route to a remote system:

```
% traceroute destination-hostname
```

You can run this form of the `traceroute` command from your user account.

Example 7-17 Using the `traceroute` Command to Show the Route to a Remote Host

The following output from the `traceroute` command shows the seven-hop path a packet follows from the local system `nearhost` to the remote system `farhost`. The output also shows the times for a packet to traverse each hop.

```
istanbul% traceroute farhost.faraway.com
traceroute to farhost.faraway.com (172.16.64.39), 30 hops max, 40 byte packets
 1 frbldg7c-86 (172.16.86.1)  1.516 ms  1.283 ms  1.362 ms
 2 bldg1a-001 (172.16.1.211)  2.277 ms  1.773 ms  2.186 ms
 3 bldg4-bldg1 (172.16.4.42)  1.978 ms  1.986 ms  13.996 ms
 4 bldg6-bldg4 (172.16.4.49)  2.655 ms  3.042 ms  2.344 ms
 5 ferbldg11a-001 (172.16.1.236)  2.636 ms  3.432 ms  3.830 ms
 6 frbldg12b-153 (172.16.153.72)  3.452 ms  3.146 ms  2.962 ms
 7 sanfrancisco (172.16.64.39)  3.430 ms  3.312 ms  3.451 ms
```

▼ How to Trace All Routes

This procedure uses the `-a` option of the `traceroute` command to trace all routes.

Step ● Type the following command on the local system:

```
% traceroute -a host-name
```

You can run this form of the `traceroute` command from your user account.

Example 7-18 Tracing All Routes to a Dual-Stack Host

This example shows all possible routes to a dual-stack host.

```
% traceroute -a v6host.remote.com
traceroute: Warning: Multiple interfaces found; using 2::56:a0:a8 @ eri0:2
traceroute to v6host (2001:db8:4a3b::102:a0:fe79:19b0), 30 hops max, 60 byte packets
 1 v6-rout86 (2001:db8:4a3b:56:a0:fe1f:59a1)  35.534 ms  56.998 ms *
 2 2001:db8::255:0:c0a8:717  32.659 ms  39.444 ms *
 3 farhost.faraway.COM (2001:db8:4a3b::103:a0:fe9a:ce7b)  401.518 ms  7.143 ms *
 4 distant.remote.com (2001:db8:4a3b::100:a0:fe7c:cf35)  113.034 ms  7.949 ms *
 5 v6host (2001:db8:4a3b::102:a0:fe79:19b0)  66.111 ms *  36.965 ms

traceroute to v6host.remote.com (192.168.10.75), 30 hops max, 40 byte packets
```

```
1 v6-rout86 (172.16.86.1) 4.360 ms 3.452 ms 3.479 ms
2 flrmpj17u.here.COM (172.16.17.131) 4.062 ms 3.848 ms 3.505 ms
3 farhost.farway.com (10.0.0.23) 4.773 ms * 4.294 ms
4 distant.remote.com (192.168.10.104) 5.128 ms 5.362 ms *
5 v6host (192.168.15.85) 7.298 ms 5.444 ms *
```

Monitoring Packet Transfers With the snoop Command

You can use the `snoop` command to monitor the state of data transfers. `snoop` captures network packets and displays their contents in the format that you specify. Packets can be displayed as soon as they are received, or saved to a file. When `snoop` writes to an intermediate file, packet loss under busy trace conditions is unlikely. `snoop` itself is then used to interpret the file.

To capture packets to and from the default interface in promiscuous mode, you must assume the Network Management role or become superuser. In summary form, `snoop` displays only the data that pertains to the highest-level protocol. For example, an NFS packet only displays NFS information. The underlying RPC, UDP, IP, and Ethernet frame information is suppressed but can be displayed if either of the verbose options is chosen.

Use `snoop` frequently and consistently to become familiar with normal system behavior. For assistance in analyzing packets, look for a recent white paper and RFC, and seek the advice of an expert in a particular area, such as NFS or NIS. For details on using `snoop` and its options, refer to the `snoop(1M)` man page.

▼ How to Check Packets From All Interfaces

Steps 1. **On the local host, assume the Network Management role or become superuser.**

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Print information about the interfaces that are attached to the system.**

```
# ifconfig -a
```

The `snoop` command normally uses the first non-loopback device, typically the primary network interface.

3. **Begin packet capture by typing `snoop` without arguments, as shown in [Example 7-19](#)**

4. Use Control-C to halt the process.

Example 7–19 Output From the snoop Command

The basic snoop command returns output that resembles the following, for a dual-stack host.

```
% snoop
Using device /dev/hme (promiscuous mode)
farhost.remote.com -> myhost          RLOGIN C port=993
  myhost -> farhost.remote.com        RLOGIN R port=993 Using device /dev/hme
router5.local.com -> router5.local.com ARP R 10.0.0.13, router5.local.com is
  0:10:7b:31:37:80
router5.local.com -> BROADCAST        TFTP Read "network-config" (octet)
farhost.remote.com -> myhost          RLOGIN C port=993
  myhost -> nisserve2                 NIS C MATCH 10.0.0.64 in ipnodes.byaddr
nisserve2 -> myhost                   NIS R MATCH No such key
  blue-112 -> slave-253-2             NIS C MATCH 10.0.0.112 in ipnodes.byaddr
myhost -> DNSserver.local.com         DNS C 192.168.10.10.in-addr.arpa. Internet PTR ?
DNSserver.local.com myhost           DNS R 192.168.10.10.in-addr.arpa. Internet PTR nisserve2.
.
.
farhost.remote.com-> myhost           RLOGIN C port=993
  myhost -> farhost.remote.com        RLOGIN R port=993 fe80::a00:20ff:febb:
.
fe80::a00:20ff:febb:e09 -> ff02::9 RIPng R (5 destinations)
```

The packets that are captured in this output show a remote login session, including lookups to the NIS and DNS servers for address resolution. Also included are periodic ARP packets from the local router and advertisements of the IPv6 link-local address to in.rpnpd.

▼ How to Capture snoop Output Into a File

Steps 1. On the local host, assume the Network Management role or become superuser.

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. Capture a snoop session into a file.

```
# snoop -o filename
```

For example:

```
# snoop /tmp/cap
Using device /dev/eri (promiscuous mode)
30 snoop: 30 packets captured
```

In the example, 30 packets have been captured in a file named /tmp/cap. The file can be in any directory with enough disk space. The number of packets that are

captured is displayed on the command line, enabling you to press Control-C to abort at any time.

snoop creates a noticeable networking load on the host machine, which can distort the results. To see the actual results, run snoop from a third system.

3. Inspect the snoop output captures file.

```
# snoop -i filename
```

Example 7-20 Contents of a snoop Output Captures File

The following output shows a variety of captures such as you might receive as output from the snoop -i command.

```
# snoop -i /tmp/cap
1 0.00000 fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fe8d:4375
   ICMPv6 Neighbor advertisement
2 0.16198 farhost.com -> myhost RLOGIN C port=985
3 0.00008 myhost -> farhost.com RLOGIN R port=985
10 0.91493 10.0.0.40 -> (broadcast) ARP C Who is 10.0.0.40, 10.0.0.40 ?
34 0.43690 nearserver.here.com -> 224.0.1.1 IP D=224.0.1.1 S=10.0.0.40 LEN=28,
   ID=47453, TO =0x0, TTL=1
35 0.00034 10.0.0.40 -> 224.0.1.1 IP D=224.0.1.1 S=10.0.0.40 LEN=28, ID=57376,
   TOS=0x0, TTL=47
```

▼ How to Check Packets Between an IPv4 Server and a Client

Steps 1. Establish a snoop system off a hub that is connected to either the client or the server.

The third system (the snoop system) checks all the intervening traffic, so the snoop trace reflects what is actually happening on the wire.

2. On the snoop system, assume the Network Management role or become superuser.

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

3. Type snoop with options and save the output to a file.

4. Inspect and interpret the output.

Refer to RFC 1761, Snoop Version 2 Packet Capture File Format (<http://www.ietf.org/rfc/rfc1761.txt?number=1761>) for details of the snoop capture file.

▼ How to Monitor IPv6 Network Traffic

You can use the `snoop` command to display only IPv6 packets.

- Steps**
1. **On the local node, assume the Network Management role or become superuser.**
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Capture IPv6 packets.**

```
# snoop ip6
```

For more information on the `snoop` command, see the `snoop(1M)` man page.

Example 7–21 Displaying Only IPv6 Network Traffic

The following example shows typical output such as you might receive from running the `snoop ip6` command on a node.

```
# snoop ip6
fe80::a00:20ff:fe9:2d27 -> ff02::1:ffe9:2d27 ICMPv6 Neighbor solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:febb:e09 -> ff02::9 RIPng R (11 destinations)
fe80::a00:20ff:fee9:2d27 -> ff02::1:ffcd:4375 ICMPv6 Neighbor solicitation
```

Administering Default Address Selection

The Solaris OS enables a single interface to have multiple IP addresses. For example, technologies, such as network multipathing (IPMP) enable multiple network interface cards (NICs) to connect to the same IP link layer. That link can have one or more IP addresses. Additionally, interfaces on IPv6-enabled systems have a link-local IPv6 address, at least one IPv6 routing address, and an IPv4 address for at least one interface.

When the system initiates a transaction, an application makes a call to the `getaddrinfo` socket. `getaddrinfo` discovers the possible address in use on the destination system. The kernel then prioritizes this list to find the best destination to use for the packet. This process is called *destination address ordering*. The Solaris kernel then selects the appropriate format for the source address, given the best destination address for the packet. The process is known as *address selection*. For more information on destination address ordering, see the `getaddrinfo(3SOCKET)` man page.

Both IPv4-only and dual-stack IPv4/IPv6 systems must perform default address selection. In most circumstances, you do not need to change the default address selection mechanisms. However, you might need to change the priority of address formats to support IPMP or to prefer 6to4 address formats, for example.

▼ How to Administer the IPv6 Address Selection Policy Table

The following procedure explains how to modify the address selection policy table. For conceptual information about IPv6 default address selection, refer to [“ipaddrsel Command” on page 216](#).



Caution – Do not change the IPv6 address selection policy table, except for the reasons shown in the next task. You can cause problems on the network with a badly constructed policy table. Be sure to save a backup copy of the policy table, as is done in the next procedure.

Steps 1. Assume the Primary Administrator role, or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Review the current IPv6 address selection policy table.

```
# ipaddrsel
# Prefix                Precedence Label
::1/128                 50 Loopback
::/0                    40 Default
2002::/16               30 6to4
::/96                   20 IPv4_Compatible
::ffff:0.0.0.0/96      10 IPv4
```

3. Make a backup copy of the default address policy table.

```
# cp /etc/inet/ipaddrsel.conf /etc/inet/ipaddrsel.conf.orig
```

4. Use a text editor to add your customizations to `/etc/inet/ipaddrsel.conf`.

Use the following syntax for entries in `/etc/inet/ipaddrsel`:

```
prefix/prefix-length precedence label [# comment ]
```

Here are some common modifications that you might want to make to your policy table:

- Give the highest priority to 6to4 addresses.

```
2002::/16                50 6to4
::1/128                  45 Loopback
```

The 6to4 address format now has the highest priority, 50. Loopback, which previously had a 50 precedence, now has a 45 precedence. The other addressing formats remain the same.

- Designate a specific source address to be used in communications with a specific destination address.

```

::1/128                50 Loopback
2001:1111:1111::1/128 40 ClientNet
2001:2222:2222::/48   40 ClientNet
::/0                  40 Default

```

This particular entry is useful for hosts with only one physical interface. Here `2001:1111:1111::1/128` is preferred as the source address on all packets that are bound for destinations within network `2001:2222:2222::/48`. The 40 priority gives higher precedence to the source address `2001:1111:1111::1/128` than to other address formats configured for the interface.

- Favor IPv4 addresses over IPv6 addresses.

```

::ffff:0.0.0.0/96     60 IPv4
::1/128               50 Loopback
.
.

```

The IPv4 format `::ffff:0.0.0.0/96` has its precedence changed from the default 10 to 60, the highest priority in the table.

5. Load the modified policy table into the kernel.

```
ipaddrsel -f /etc/inet/ipaddrsel.conf
```

6. If the modified policy table has problems, restore the default IPv6 address selection policy table.

```
# ipaddrsel -d
```

▼ How to Modify the IPv6 Address Selection Table for the Current Session Only

When you edit the `/etc/inet/ipaddrsel.conf`, file, any modifications that you make persist across reboots. If you want the modified policy table to exist only in the current session, follow this procedure.

Steps 1. Assume the Primary Administrator role, or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Copy the contents of `/etc/inet/ipaddrsel` into *filename*, where *filename* represents a name of your choice.

```
# cp /etc/inet/ipaddrsel filename
```

3. Edit the policy table in *filename* to your specifications.

4. Load the modified policy table into the kernel.

```
# ipaddrsel -f filename
```

The kernel uses the new policy table until you reboot the system.

Troubleshooting Network Problems (Tasks)

This chapter contains solutions for common problems that might occur on your network. The following topics are covered:

- “General Network Troubleshooting Tips” on page 177
- “Common Problems When Deploying IPv6” on page 179

General Network Troubleshooting Tips

One of the first signs of trouble on a network is a loss of communications by one or more hosts. If a host does not come up at all the first time that the host is added to the network, the problem might be in one of the configuration files. The problem might also be a faulty network interface card. If a single host suddenly develops a problem, the network interface might be the cause. If the hosts on a network can communicate with each other but not with other networks, the problem could lie with the router. Or, the problem could be in another network.

You can use the `ifconfig` command to obtain information on network interfaces. Use the `netstat` command to display routing tables and protocol statistics. Third-party network diagnostic programs provide a number of troubleshooting tools. Refer to third-party documentation for information.

Less obvious are the causes of problems that degrade performance on the network. For example, you can use tools such as `ping` to quantify problems such as the loss of packets by a host.

Running Basic Diagnostic Checks

If the network has problems, you can run a series of software checks to diagnose and fix basic, software-related problems.

▼ How to Perform Basic Network Software Checking

- Steps**
- 1. On the local system, assume the Network Management role or become superuser.**
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.
 - 2. Use the `netstat` command to display network information.**
For syntax and information about the `netstat` command, refer to “Monitoring Network Status With the `netstat` Command” on page 157 and the `netstat(1M)` man page.
 - 3. Check the `hosts` database (and `ipnodes` database, if you are using IPv6) to ensure that the entries are correct and current.**
For information about the `/etc/inet/hosts` database, refer to “`hosts Database`” on page 185 and the `hosts(4)` man page. For information about the `/etc/inet/ipnodes` database, refer to “`ipnodes Database`” on page 241 and the `ipnodes(4)` man page.
 - 4. If you are running the Reverse Address Resolution Protocol (RARP), check the Ethernet addresses in the `ethers` database to ensure that the entries are correct and current.**
 - 5. Try to connect to the local host by using the `telnet` command.**
For syntax and information about `telnet`, refer to the `telnet(1)` man page.
 - 6. Ensure that the network daemon `inetd` is running.**

```
# ps -ef | grep inetd
```

The following output verifies that the `inetd` daemon is running:

```
root 57 1 0 Apr 04 ? 3:19 /usr/sbin/inetd -s
```
 - 7. If IPv6 is enabled on your network, verify that the IPv6 daemon `in.ndpd` is running:**

```
# ps -ef | grep in.ndpd
```

The following output verifies that the `in.ndpd` daemon is running:

```
root 123 1 0 Oct 27 ? 0:03 /usr/lib/inet/in.ndpd
```

Common Problems When Deploying IPv6

This section describes issues and problems that you might encounter while planning and deploying IPv6 at your site. For actual planning tasks, refer to [Chapter 4](#).

IPv4 Router Cannot Be Upgraded to IPv6

If your existing equipment cannot be upgraded, you might have to purchase IPv6-ready equipment. Check the manufacturers' documentation for any equipment-specific procedures you might have to perform to support IPv6.

Certain IPv4 routers cannot be upgraded for IPv6 support. If this situation applies to your topology, physically wire an IPv6 router next to the IPv4 router. Then, you can tunnel from the IPv6 router over the IPv4 router. For tasks for configuring tunnels, refer to "[Tasks for Configuring Tunnels for IPv6 Support \(Task Map\)](#)" on page 129.

Problems After Upgrading Services to IPv6

You might encounter the following situations when preparing services for IPv6 support:

- Certain applications, even after they are ported to IPv6, do not turn on IPv6 support by default. You might have to configure these applications to turn on IPv6.
- A server that runs multiple services, some of which are IPv4 only, and others that are both IPv4 and IPv6, can experience problems. Some clients might need to use both types of services, which leads to confusion on the server side.

Current ISP Does Not Support IPv6

If you want to deploy IPv6 but your current ISP does not offer IPv6 addressing, consider the following alternatives to changing ISPs:

- Hire an ISP to provide a second line for IPv6 communications from your site. This solution is expensive.
- Get a *virtual ISP*. A virtual ISP provides your site with IPv6 connectivity but no link. Instead, you create a tunnel from your site, over your IPv4 ISP, to the virtual ISP.
- Use a 6to4 tunnel over your ISP to other IPv6 sites. For an address, use the registered IPv4 address of the 6to4 router as the public topology part of the IPv6 address.

Security Issues When Tunneling to a 6to4 Relay Router

By nature, a tunnel between a 6to4 router and a 6to4 relay router is insecure. Security problems, such as the following, are inherent in such a tunnel:

- Though 6to4 relay routers do encapsulate and decapsulate packets, these routers do not check the data that is contained within the packets.
- Address spoofing is a major issue on tunnels to a 6to4 relay router. For incoming traffic, the 6to4 router is unable to match the IPv4 address of the relay router with the IPv6 address of the source. Therefore, the address of the IPv6 host can easily be spoofed. The address of the 6to4 relay router can also be spoofed.
- By default, no trust mechanism exists between 6to4 routers and 6to4 relay routers. Thus, a 6to4 router cannot identify whether the 6to4 relay router is to be trusted, or even if it is a legitimate 6to4 relay router. A trust relationship between the 6to4 site and the IPv6 destination must exist, or both sites leave themselves open to possible attacks.

These problems and other security issues that are inherent with 6to4 relay routers are explained in the Internet Draft, *Security Considerations for 6to4*. Generally, you should consider enabling support for 6to4 relay routers for the following reasons only:

- Your 6to4 site intends to communicate with a private, trusted IPv6 network. For example, you might enable 6to4 relay router support on a campus network that consists of isolated 6to4 sites and native IPv6 sites.
- Your 6to4 site has a compelling business reason to communicate with certain native IPv6 hosts.
- You have implemented the checks and trust models that are suggested in the Internet Draft, *Security Considerations for 6to4*.

Known Issues With a 6to4 Router

The following known bugs affect 6to4 configuration:

- 4709338 – Need a RIPng implementation which recognizes static routes
- 4152864 – Configuring two tunnels with the same tsrc/tdst pair works

Implementing Static Routes at the 6to4 Site (Bug ID 4709338)

The following issue occurs on 6to4 sites with routers that are internal to the 6to4 boundary router. When you configure the 6to4 pseudo-interface, the static route 2002::/16 is automatically added to the routing table on the 6to4 router. Bug 4709338 describes a limitation in the Solaris RIPng routing protocol that prevents this static route from being advertised to the 6to4 site.

Either of the following workarounds are available for Bug 4709338.

- Add the `2002::/16` static route to the routing tables of all intrasite routers within the 6to4 site.
- Use a routing protocol other than RIPng on the 6to4 site's internal router.

Configuring Tunnels with the Same Source Address (Bug ID 4152864)

Bug ID 4152864 describes problems that occur when two tunnels are configured with the same tunnel source address, which is a serious issue for 6to4 tunnels.



Caution – Do not configure a 6to4 tunnel and an automatic tunnel (`atun`) with the same tunnel source address. For information about automatics and the `atun` command, refer to the `tun(7M)` man page.

TCP/IP and IPv4 in Depth (Reference)

This chapter provides TCP/IP network reference information about network configuration files, including the types, their purpose, and the format of the file entries. The existing network databases are also described in detail. The chapter also shows how the structure of IPv4 addresses are derived, based on defined network classifications and subnet numbers.

This chapter contains the following information:

- “TCP/IP Configuration Files” on page 183
- “Network Databases and the `nsswitch.conf` File” on page 192
- “Routing Protocols in the Solaris OS” on page 201
- “Network Classes” on page 202

TCP/IP Configuration Files

Each system on the network obtains its TCP/IP configuration information from the following TCP/IP configuration files and network databases:

- `/etc/hostname.interface` file
- `/etc/nodename` file
- `/etc/defaultdomain` file
- `/etc/defaultrouter` file (optional)
- `hosts` database
- `ipnodes` database
- `netmasks` database (optional)

The Solaris installation program creates these files as part of the installation process. You can also edit the files manually, as explained in this section. The `hosts` and `netmasks` databases are two of the network databases read by the name services available on Solaris networks. [“Network Databases and the `nsswitch.conf` File” on page 192](#) describes in detail the concept of network databases. For information on the `ipnodes` file, see [“ipnodes Database” on page 241](#).

`/etc/hostname.interface` File

This file defines the physical network interfaces on the local host. At least one `/etc/hostname.interface` file should exist on the local system. The Solaris installation program creates an `/etc/hostname.interface` file for the first interface that is found during the installation process. This interface usually has the lowest device number, for example `eri0`, and is referred to as the *primary network interface*. If the installation programs finds additional interfaces, you optionally can configure them, as well, as part of the installation process.

If you add a new network interface to your system after installation, you must create an `/etc/hostname.interface` file for that interface, as explained in [“How to Add a Physical Interface After Installation” on page 113](#). Also, for the Solaris software to recognize and use the new network interface, you need to load the interface’s device driver into the appropriate directory. Refer to the documentation that comes with the new network interface for the appropriate *interface* name and device driver instructions.

The basic `/etc/hostname.interface` file contains one entry: the host name or IPv4 address that is associated with the network interface. For example, suppose `smc0` is the primary network interface for a system that is called `tenere`. The `/etc/hostname.interface` file would have the name `/etc/hostname.smc0`. The file would contain the entry `tenere`.

Note – IPv6 uses the `/etc/hostname6.interface` file for defining network interfaces. For more information, refer to [“IPv6 Interface Configuration File” on page 215](#).

`/etc/nodename` File

This file should contain one entry: the host name of the local system. For example, on system `timbuktu`, the file `/etc/nodename` would contain the entry `timbuktu`.

`/etc/defaultdomain` File

This file should contain one entry: the fully qualified domain name of the administrative domain to which the local host's network belongs. You can supply this name to the Solaris installation program or edit the file at a later date. For more information on network domains, refer to *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

`/etc/defaultrouter` File

This file can contain an entry for each router that is directly connected to the network. The entry should be the name for the network interface that functions as a router between networks. The presence of the `/etc/defaultrouter` file indicates that the system is configured to support static routing.

hosts Database

The `hosts` database contains the IPv4 addresses and host names of systems on your network. If you use the NIS or DNS name service, or the LDAP directory service, the `hosts` database is maintained in a database that is designated for host information. For example, on a network that runs NIS, the `hosts` database is maintained in the `hostsbyname` file.

If you use local files for the name service, the `hosts` database is maintained in the `/etc/inet/hosts` file. This file contains the host names and IPv4 addresses of the primary network interface, other network interfaces that are attached to the system, and any other network addresses that the system must check for.

Note – For compatibility with BSD-based operating systems, the `/etc/hosts` file is a symbolic link to `/etc/inet/hosts`.

`/etc/inet/hosts` File Format

The `/etc/inet/hosts` file uses the basic syntax that follows. Refer to the `hosts(4)` man page for complete syntax information.

IPv4-address hostname [nicknames] [#comment]

IPv4-address Contains the IPv4 address for each interface that the local host must recognize.

hostname Contains the host name that is assigned to the system at setup, plus the host names that are assigned to additional network interfaces that the local host must recognize.

- [*nickname*] Is an optional field that contains a nickname for the host.
- [*#comment*] Is an optional field for a comment.

Initial `/etc/inet/hosts` File

When you run the Solaris installation program on a system, the program configures the initial `/etc/inet/hosts` file. This file contains the minimum entries that the local host requires. The entries include the loopback address, the host IPv4 address, and the host name.

For example, the Solaris installation program might create the following `/etc/inet/hosts` file for system `tenere` shown in [Figure 5-1](#):

EXAMPLE 9-1 `/etc/inet/hosts` File for System `tenere`

```
127.0.0.1    localhost      loghost      #loopback address
192.168.200.3  tenere          #host name
```

Loopback Address

In [Example 9-1](#), the IPv4 address `127.0.0.1` is the *loopback address*. The loopback address is the reserved network interface that is used by the local system to allow interprocess communication. This address enables the host to send packets to itself. The `ifconfig` command uses the loopback address for configuration and testing, as explained in “[Monitoring the Interface Configuration With the `ifconfig` Command](#)” on [page 153](#). Every system on a TCP/IP network must use the IP address `127.0.0.1` for IPv4 loopback on the local host.

Host Name

The IPv4 address `192.168.200.1` and the name `tenere` are the address and host name of the local system. They are assigned to the system’s primary network interface.

Multiple Network Interfaces

Some systems have more than one network interface, because they are either routers or multihomed hosts. Each network interface that is attached to the system requires its own IP address and associated name. During installation, you must configure the primary network interface. If a particular system has multiple interfaces at installation time, the Solaris installation program also prompts you about these additional interfaces. You can optionally configure one or more additional interfaces at this time, or manually, at a later date.

After Solaris installation, you can configure additional interfaces for a router or multihomed host by adding interface information to the systems' `/etc/inet/hosts` file. For more information on configuring routers and multihomed hosts refer to "Configuring a Router" on page 118 and "Multihomed Hosts" on page 121.

Example 9-2 shows the `/etc/inet/hosts` file for system `timbuktu` that is shown in Figure 5-1.

EXAMPLE 9-2 `/etc/inet/hosts` File for System `timbuktu`

```
127.0.0.1      localhost    loghost
192.168.200.70 timbuktu     #This is the local host name
192.168.201.10 timbuktu-201 #Interface to network 192.9.201
```

With these two interfaces, `timbuktu` connects networks `192.168.200` and `192.168.201` as a router.

How Name Services Affect the `hosts` Database

The NIS and DNS name services, and LDAP directory service, maintain host names and addresses on one or more servers. These servers maintain `hosts` databases that contain information for every host and router (if applicable) on the servers' network. Refer to *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* for more information about these services.

When Local Files Provide the Name Service

On a network that uses local files for the name service, systems that run in local files mode consult their individual `/etc/inet/hosts` files for IPv4 addresses and host names of other systems on the network. Therefore, these system's `/etc/inet/hosts` files must contain the following:

- Loopback address
- IPv4 address and host name of the local system (primary network interface)
- IPv4 address and host name of additional network interfaces that are attached to this system, if applicable
- IPv4 addresses and host names of all hosts on the local network
- IPv4 addresses and host names of any routers that this system must know about, if applicable
- IPv4 address of any system your system wants to refer to by its host name

Figure 9-1 shows the `/etc/inet/hosts` file for system `tenere`. This system runs in local files mode. Notice that the file contains the IPv4 addresses and host names for every system on the `192.9.200` network. The file also contains the IPv4 address and interface name `timbuktu-201`. This interface connects the `192.9.200` network to the `192.9.201` network.

A system that is configured as a network client uses the local `/etc/inet/hosts` file for its loopback address and IPv4 address.

```

# Desert Network - Hosts File
#
# If the NIS is running, this file is only consulted
# when booting
#
Localhost Line --- 127.0.0.1 localhost
#
Host Name Line --- 192.9.200.1  tenere                #This is my machine
#
Server Line --- 192.9.200.50  sahara                big          #This is the net config server
#
#
Other Hosts --- 192.9.200.2  libyan                libby       #This is Tom's machine
                192.9.200.3  ahaggar                #This is Bob's machine
                192.9.200.4  nubian                #This is Amina's machine
                192.9.200.5  faiyum                suz         #This is Suzanne's machine
                192.9.200.70  timbuktu              tim         #This is Kathy's machine
                192.9.201.10  timbuktu-201          #Interface to net 192.9.201 on
                #timbuktu

```

FIGURE 9-1 `/etc/inet/hosts` File for a System Running in Local Files Mode

netmasks Database

You need to edit the `netmasks` database as part of network configuration *only* if you have set up subnetting on your network. The `netmasks` database consists of a list of networks and their associated subnet masks.

Note – When you create subnets, each new network must be a separate physical network. You cannot apply subnetting to a single physical network.

What Is Subnetting?

Subnetting is a method for maximizing the limited 32-bit IPv4 addressing space and reducing the size of the routing tables in a large internetwork. With any address class, subnetting provides a means of allocating a part of the host address space to network addresses, which lets you have more networks. The part of the host address space that is allocated to new network addresses is known as the *subnet number*.

In addition to making more efficient use of the IPv4 address space, subnetting has several administrative benefits. Routing can become very complicated as the number of networks grows. A small organization, for example, might give each local network a class C number. As the organization grows, the administration of a number of different network numbers could become complicated. A better idea is to allocate a few class B network numbers to each major division in an organization. For example, you could allocate one Class B network to Engineering, one Class B to Operations, and so on. Then, you could divide each class B network into additional networks, using the additional network numbers gained by subnetting. This division can also reduce the amount of routing information that must be communicated among routers.

Creating the Network Mask for IPv4 Addresses

As part of the subnetting process, you need to select a network-wide *netmask*. The netmask determines how many and which bits in the host address space represent the subnet number and how many and which bits represent the host number. Recall that the complete IPv4 address consists of 32 bits. Depending on the address class, as many as 24 bits and as few as 8 bits can be available for representing the host address space. The netmask is specified in the `netmasks` database.

If you plan to use subnets, you must determine your netmask before you configure TCP/IP. If you plan to install the operating system as part of network configuration, the Solaris installation program requests the netmask for your network.

As described in [“Designing an IPv4 Addressing Scheme” on page 57](#), 32-bit IP addresses consist of a network part and a host part. The 32 bits are divided into 4 bytes. Each byte is assigned to either the network number or the host number, depending on the network class.

For example, in a class B IPv4 address, the 2 bytes on the left are assigned to the network number, and the 2 bytes on the right are assigned to the host number. In the class B IPv4 address 172.16.10, you can assign the 2 bytes on the right to hosts.

If you are to implement subnetting, you need to use some of the bits in the bytes that are assigned to the host number to apply to subnet addresses. For example, a 16-bit host address space provides addressing for 65,534 hosts. If you apply the third byte to subnet addresses and the fourth byte to host addresses, you can address up to 254 networks, with up to 254 hosts on each network.

The bits in the host address bytes that are applied to subnet addresses and those applied to host addresses are determined by a *subnet mask*. Subnet masks are used to select bits from either byte for use as subnet addresses. Although netmask bits must be contiguous, they need not align on byte boundaries.

The netmask can be applied to an IPv4 address by using the bitwise logical AND operator. This operation selects out the network number and subnet number positions of the address.

Netmasks can be explained in terms of their binary representation. You can use a calculator for binary-to-decimal conversion. The following examples show both the decimal and binary forms of the netmask.

If a netmask 255.255.255.0 is applied to the IPv4 address 172.16.41.101, the result is the IPv4 address of 172.16.41.0.

172.16.41.101 & 255.255.255.0 = 172.16.41.0

In binary form, the operation is as follows:

10000001.10010000.00101001.01100101 (IPv4 address)

ANDed with

11111111.11111111.11111111.00000000 (netmask)

Now the system looks for a network number of 172.16.41 instead of a network number of 172.16. If your network has the number 172.16.41, that number is what the system checks for and finds. Because you can assign up to 254 values to the third byte of the IPv4 address space, subnetting lets you create address space for 254 networks, where previously space was available for only one.

If you are providing address space for only two additional networks, you can use the following subnet mask:

255.255.192.0

This netmask provides the following result:

11111111.11111111.11000000.00000000

This result still leaves 14 bits available for host addresses. Because all 0s and 1s are reserved, at least 2 bits must be reserved for the host number.

/etc/inet/netmasks File

If your network runs NIS or LDAP, the servers for these name services maintain netmasks databases. For networks that use local files for the name service, this information is maintained in the `/etc/inet/netmasks` file.

Note – For compatibility with BSD-based operating systems, the `/etc/netmasks` file is a symbolic link to `/etc/inet/netmasks`.

The following example shows the `/etc/inet/netmasks` file for a class B network.

EXAMPLE 9-3 /etc/inet/netmasks File for a Class B Network

```
# The netmasks file associates Internet Protocol (IPv4) address
# masks with IPv4 network numbers.
#
#   network-number   netmask
#
# Both the network-number and the netmasks are specified in
# "decimal dot" notation, e.g:
#
#           128.32.0.0   255.255.255.0
192.168.0.0  255.255.255.0
```

If the `/etc/netmasks` file does not exist, create it with a text editor. Use the following syntax:

```
network-number netmask-number
```

Refer to the `netmasks(4)` man page for complete details.

When creating netmask numbers, type the network number that is assigned by the ISP or Internet Registry (not the subnet number) and the netmask number in `/etc/inet/netmasks`. Each subnet mask should be on a separate line.

For example:

```
128.78.0.0           255.255.248.0
```

You can also type symbolic names for network numbers in the `/etc/inet/hosts` file. You can then use these network names instead of the network numbers as parameters to commands.

inetd Internet Services Daemon

The `inetd` daemon starts up Internet standard services when a system boots, and can restart a service while a system is running. Use the Service Management Facility (SMF) to modify the standard Internet services or to have additional services started by the `inetd` daemon.

Use the following SMF commands to manage services started by `inetd`:

- | | |
|----------------------|--|
| <code>svcadm</code> | For administrative actions on a service, such as enabling, disabling, or restarting. For details, refer to the <code>svcadm(1M)</code> man page. |
| <code>svcs</code> | For querying the status of a service. For details, refer to the <code>svcs(1)</code> man page. |
| <code>inetadm</code> | For displaying and modifying the properties of a service. For details, refer to the <code>inetadm(1M)</code> man page. |

The `proto` field value in the `inetadm` profile for a particular service indicates the transport layer protocol on which the service runs. If the service is IPv4-only, the `proto` field must be specified as `tcp`, `udp`, or `sctp`.

- For instructions on using the SMF commands, refer to “SMF Command-Line Administrative Utilities” in *System Administration Guide: Basic Administration*.
- For a task that uses the SMF commands to add a service that runs over SCTP, refer to “[How to Add Services That Use the SCTP Protocol](#)” on page 109.
- For information on adding services that handle both IPv4 requests and IPv6 requests, refer to “[inetd Internet Services Daemon](#)” on page 192

Network Databases and the `nsswitch.conf` File

The network databases are files that provide information that is needed to configure the network. The network databases follow:

- `hosts`
- `ipnodes`
- `netmasks`
- `ethers` database
- `bootparams`
- `protocols`

- `services`
- `networks`

As part of the configuration process, you edit the `hosts` database and the `netmasks` database, if your network is subnetted. Two network databases, `bootparams` and `ethers`, are used to configure systems as network clients. The remaining databases are used by the operating system and seldom require editing.

Although `nsswitch.conf` file is not a network database, you need to configure this file along with the relevant network databases. `nsswitch.conf` specifies which name service to use for a particular system: local files, NIS, DNS, or LDAP.

How Name Services Affect Network Databases

The format of your network database depends on the type of name service you select for your network. For example, the `hosts` database contains, at least the host name and IPv4 address of the local system and any network interfaces that are directly connected to the local system. However, the `hosts` database could contain other IPv4 addresses and host names, depending on the type of name service on your network.

The network databases are used as follows:

- Networks that use local files for their name service rely on files in the `/etc/inet` and `/etc` directories.
- NIS uses databases that are called NIS maps.
- DNS uses records with host information.

Note – DNS boot and data files do not correspond directly to the network databases.

The following figure shows the forms of the `hosts` database that are used by these name services.

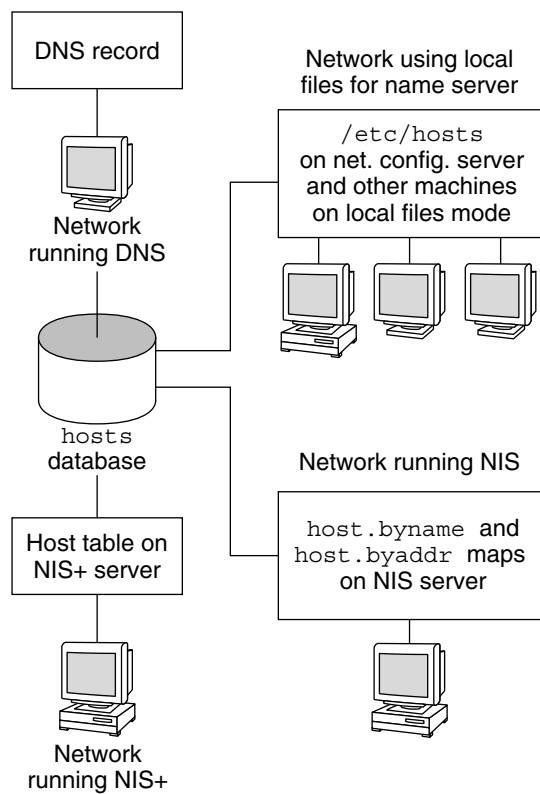


FIGURE 9-2 Forms of the `hosts` Database Used by Name Services

The following table lists the network databases and their corresponding local files and NIS maps

TABLE 9-1 Network Databases and Corresponding Name Service Files

Network Database	Local Files	NIS Maps
<code>hosts</code>	<code>/etc/inet/hosts</code>	<code>hosts.byaddr</code> <code>hosts.byname</code>
<code>ipnodes</code>	<code>/etc/inet/ipnodes</code>	<code>ipnodes.byaddr</code> <code>ipnodes.byname</code>
<code>netmasks</code>	<code>/etc/inet/netmasks</code>	<code>netmasks.byaddr</code>
<code>ethers</code>	<code>/etc/ethers</code>	<code>ethers.byname</code> <code>ethers.byaddr</code>
<code>bootparams</code>	<code>/etc/bootparams</code>	<code>bootparams</code>
<code>protocols</code>	<code>/etc/inet/protocols</code>	<code>protocols.byname</code> <code>protocols.bynumber</code>
<code>services</code>	<code>/etc/inet/services</code>	<code>services.byname</code>

TABLE 9-1 Network Databases and Corresponding Name Service Files (Continued)

Network Database	Local Files	NIS Maps
networks	/etc/inet/networks	networks.byaddr networks.byname

This book discusses network databases as they are viewed by networks that use local files for name services.

- Information about the `hosts` database is in “[hosts Database](#)” on page 185.
- Information about the `netmasks` database is in “[netmasks Database](#)” on page 188.
- Information about the `ipnodes` database is in “[ipnodes Database](#)” on page 241.

Refer to *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)* for information on network databases correspondences in NIS, DNS, and LDAP.

nsswitch.conf File

The `/etc/nsswitch.conf` file defines the search order of the network databases. The Solaris installation program creates a default `/etc/nsswitch.conf` file for the local system, based on the name service you indicate during the installation process. If you selected the “None” option, indicating local files for name service, the resulting `nsswitch.conf` file resembles the following example.

EXAMPLE 9-4 `nsswitch.conf` for Networks Using Files for Name Service

```
# /etc/nsswitch.conf:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it does not use any naming service.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file contains "switch.so" as a
# nametoaddr library for "inet" transports.

passwd:      files
group:       files
hosts:       files
networks:    files
protocols:   files
rpc:         files
ethers:      files
netmasks:   files
bootparams:  files
publickey:   files
# At present there isn't a 'files' backend for netgroup; the
# system will figure it out pretty quickly,
# and won't use netgroups at all.
```

EXAMPLE 9-4 `nsswitch.conf` for Networks Using Files for Name Service (Continued)

```
netgroup:      files
automount:    files
aliases:      files
services:     files
sendmailvars: files
```

The `nsswitch.conf(4)` man page describes the file in detail. The basic syntax is shown here:

database name-service-to-search

The *database* field can list one of many types of databases that are searched by the operating system. For example, the field could indicate a database that affects users, such as `passwd` or `aliases`, or a network database. The parameter *name-service-to-search* can have the values `files`, `nis`, or `nis+` for the network databases. The `hosts` database can also have `dns` as a name service to search. You can also list more than one name service, such as `nis+` and `files`.

In [Example 9-4](#), the only search option that is indicated is `files`. Therefore, the local system obtains security and automounting information, in addition to network database information, from files that are located in its `/etc` and `/etc/inet` directories.

Changing `nsswitch.conf`

The `/etc` directory contains the `nsswitch.conf` file that is created by the Solaris installation program. This directory also contains template files for the following name services:

- `nsswitch.files`
- `nsswitch.nis`
- `nsswitch.nis+`

If you want to change from one name service to another name service, you can copy the appropriate template to `nsswitch.conf`. You can also selectively edit the `nsswitch.conf` file, and change the default name service to search for individual databases.

For example, on a network that runs NIS, you might have to change the `nsswitch.conf` file on network clients. The search path for the `bootparams` and `ethers` databases must list `files` as the first option, and then `nis`. The following example shows the correct search paths.

EXAMPLE 9-5 `nsswitch.conf` for a Client on a Network Running NIS

```
# /etc/nsswitch.conf:#
.
```

EXAMPLE 9-5 nsswitch.conf for a Client on a Network Running NIS (Continued)

```
passwd:      files nis
group:       file nis

# consult /etc "files" only if nis is down.
hosts:       nis      [NOTFOUND=return] files
networks:    nis      [NOTFOUND=return] files
protocols:   nis      [NOTFOUND=return] files
rpc:         nis      [NOTFOUND=return] files
ethers:      files [NOTFOUND=return] nis
netmasks:    nis      [NOTFOUND=return] files
bootparams:  files [NOTFOUND=return] nis
publickey:   nis
netgroup:    nis

automount:   files nis
aliases:     files nis

# for efficient getservbyname() avoid nis
services:    files nis
sendmailvars: files
```

For complete details on the name service switch, refer to *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

bootparams Database

The bootparams database contains information that is used by systems that are configured to boot in network client mode. You need to edit this database if your network has network clients. See “[Configuring Network Clients](#)” on page 105 for the procedures. The database is built from information that is entered into the /etc/bootparams file.

The bootparams(4) man page contains the complete syntax for this database. Basic syntax is shown here:

system-name file-key-server-name:pathname

For each network client system, the entry might contain the following information: the name of the client, a list of keys, the names of servers, and path names. The first item of each entry is the name of the client system. All items but the first item are optional. An example follows.

EXAMPLE 9-6 bootparams Database

```
myclient root=myserver : /nfsroot/myclient \
swap=myserver : /nfsswap//myclient \
dump=myserver : /nfsdump/myclient
```

In this example, the term `dump=` tells client hosts not to look for a dump file.

Wildcard Entry for `bootparams`

In most instances, use the wildcard entry when editing the `bootparams` database to support clients. This entry follows:

```
* root=server:/path dump=:
```

The asterisk (*) wildcard indicates that this entry applies to all clients that are not specifically named within the `bootparams` database.

`ethers` Database

The `ethers` database is built from information that is entered into the `/etc/ethers` file. This database associates host names to their *Media Access Control* (MAC) addresses. You need to create an `ethers` database only if you are running the RARP daemon. That is, you need to create this database if you are configuring network clients.

RARP uses the file to map MAC addresses to IP addresses. If you are running the RARP daemon in `.rarpd`, you need to set up the `ethers` file and maintain this file on all hosts that are running the daemon to reflect changes to the network.

The `ethers(4)` man page contains the complete syntax for this database. The basic syntax is shown here:

```
MAC-address hostname #comment
```

```
MAC-address    MAC address of the host
```

```
hostname       Official name of the host
```

```
#comment       Any note that you want to append to an entry in the file
```

The equipment manufacturer provides the MAC address. If a system does not display the MAC address during the system booting process, see your hardware manuals for assistance.

When adding entries to the `ethers` database, ensure that host names correspond to the primary names in the `hosts` and `ipnodes` databases, not to the nicknames, as follows.

EXAMPLE 9-7 Entries in the `ethers` Database

```
8:0:20:1:40:16  fayoum
8:0:20:1:40:15  nubian
8:0:20:1:40:7   sahara        # This is a comment
8:0:20:1:40:14  tenere
```

Other Network Databases

The remaining network databases seldom need to be edited.

networks database

The `networks` database associates network names with network numbers, enabling some applications to use and display names rather than numbers. The `networks` database is based on information in the `/etc/inet/networks` file. This file contains the names of all networks to which your network connects through routers.

The Solaris installation program configures the initial `networks` database. However, if you add a new network to your existing network topology, you must update this database.

The `networks(4)` man page contains the complete syntax for `/etc/inet/networks`. The basic format is shown here:

```
network-name network-number nickname(s) #comment
```

<i>network-name</i>	Official name for the network
<i>network-number</i>	Number assigned by the ISP or Internet Registry
<i>nickname</i>	Any other name by which the network is known
<i>#comment</i>	Any note that you want to append to an entry in the file

You must maintain the `networks` file. The `netstat` program uses the information in this database to produce status tables.

A sample `/etc/networks` file follows.

EXAMPLE 9-8 /etc/networks File

```
#ident    "@(#)networks    1.4    92/07/14 SMI"    /* SVr4.0 1.1    */
#
# The networks file associates Internet Protocol (IP) network
# numbers with network names. The format of this file is:
#
#    network-name          network-number          nicnames . . .
#
# The loopback network is used only for intra-machine communication
loopback          127
#
# Internet networks
#
arpanet          10          arpa # Historical
#
# local networks
```

EXAMPLE 9-8 /etc/networks File (Continued)

```
eng 192.168.9 #engineering
acc 192.168.5 #accounting
prog 192.168.2 #programming
```

protocols Database

The protocols database lists the TCP/IP protocols that are installed on your system and their protocol numbers. The Solaris installation program automatically creates the database. This file seldom requires any administration.

The protocols(4) man page describes the syntax of this database. An example of the /etc/inet/protocols file follows.

EXAMPLE 9-9 /etc/inet/protocols File

```
#
# Internet (IP) protocols
#
ip 0 IP # internet protocol, pseudo protocol number
icmp 1 ICMP # internet control message protocol
tcp 6 TCP # transmission control protocol
udp 17 UDP # user datagram protocol
```

services Database

The services database lists the names of TCP and UDP services and their well-known port numbers. This database is used by programs that call network services. The Solaris installation automatically creates the services database. Generally, this database does not require any administration.

The services(4) man page contains complete syntax information. An excerpt from a typical /etc/inet/services file follows.

EXAMPLE 9-10 /etc/inet/services File

```
#
# Network services
#
echo 7/udp
echo 7/tcp
echo 7/sctp6
discard 9/udp sink null
discard 11/tcp
daytime 13/udp
daytime 13/tcp
```


EXAMPLE 9-10 /etc/inet/services File (Continued)

```
netstat    15/tcp
ftp-data   20/tcp
ftp        21/tcp
telnet     23/tcp
time       37/tcp    timeserver
time       37/udp    timeserver
name       42/udp    nameserver
whois      43/tcp    nickname
```

Routing Protocols in the Solaris OS

Solaris system software supports two routing protocols: Routing Information Protocol (RIP) and ICMP Router Discovery (RDISC). RIP and RDISC are both standard TCP/IP protocols.

Routing Information Protocol (RIP)

RIP is implemented by `in.routed`, the routing daemon, which automatically starts when the system boots. When run on a router with the `s` option specified, `in.routed` fills the kernel routing table with a route to every reachable network and advertises “reachability” through all network interfaces.

When run on a host with the `q` option specified, `in.routed` extracts routing information but does not advertise reachability. On hosts, routing information can be extracted in two ways:

- Do *not* specify the `S` flag (capital “S”: “Space-saving mode”). `in.routed` builds a full routing table exactly as it does on a router.
- Specify the `S` flag. `in.routed` creates a minimal kernel table, containing a single default route for each available router.

ICMP Router Discovery (RDISC) Protocol

Hosts use RDISC to obtain routing information from routers. Thus, when hosts are running RDISC, routers must also run another protocol, such as RIP, in order to exchange router information.

RDISC is implemented by `in.routed`, which should run on both routers and hosts. On hosts, `in.routed` uses RDISC to discover default routes from routers that advertise themselves through RDISC. On routers, `in.routed` uses RDISC to advertise default routes to hosts on directly-connected networks. See the `in.routed(1M)` man page and the `gateways(4)` man page.

Network Classes

Note – Class-based network numbers are no longer available from the IANA, though many older networks are still class-based.

This section provides details about IPv4 network classes. Each class uses the 32-bit IPv4 address space differently, providing more or fewer bits for the network part of the address. These classes are class A, class B, and class C.

Class A Network Numbers

A class A network number uses the first 8 bits of the IPv4 address as its “network part.” The remaining 24 bits contain the host part of the IPv4 address, as the following figure illustrates.

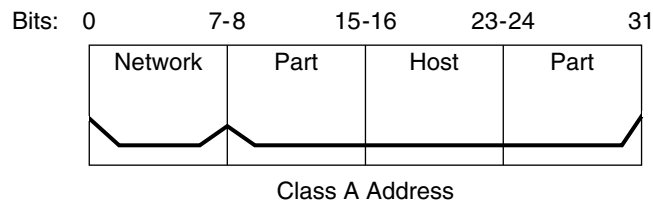


FIGURE 9-3 Byte Assignment in a Class A Address

The values that are assigned to the first byte of class A network numbers fall within the range 0–127. Consider the IPv4 address 75 . 4 . 10 . 4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4 . 10 . 4, establish the host address. Only the first byte of a class A number is registered with the IANA. Use of the remaining three bytes is left to the discretion of the owner of the network number. Only 127 class A networks exist. Each one of these numbers can accommodate a maximum of 16,777,214 hosts.

Class B Network Numbers

A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a class B network number is in the range 128–191. In the number 172 . 16 . 50 . 56, the first two bytes, 172 . 16, are registered with the IANA, and compose the network address. The last two bytes, 50 . 56, contain the host address, and are assigned at the discretion of the owner of the network number. The following figure graphically illustrates a class B address.

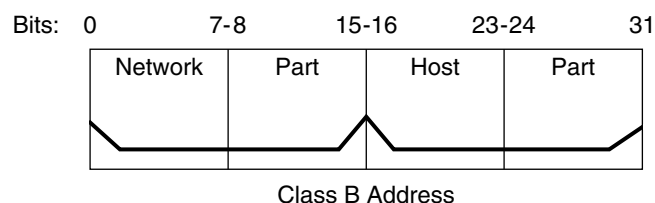


FIGURE 9-4 Byte Assignment in a Class B Address

Class B is typically assigned to organizations with many hosts on their networks.

Class C Network Numbers

Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts—the maximum being 254. A class C network number occupies the first three bytes of an IPv4 address. Only the fourth byte is assigned at the discretion of the network owners. The following figure graphically represents the bytes in a class C address.

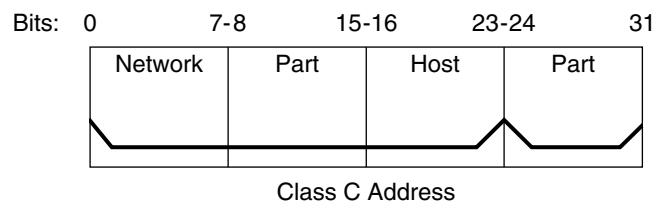


FIGURE 9-5 Byte Assignment in a Class C Address

The first byte of a class C network number covers the range 192–223. The second and third bytes each cover the range 1–255. A typical class C address might be 192 . 168 . 2 . 5. The first three bytes, 192 . 168 . 2, form the network number. The final byte in this example, 5, is the host number.

IPv6 in Depth (Reference)

This chapter contains the following reference information about the Solaris 10 IPv6 implementation.

- “IPv6 Addressing Formats Beyond the Basics” on page 205
- “IPv6 Packet Header Format” on page 208
- “Dual-Stack Protocols” on page 210
- “Solaris 10 IPv6 Implementation” on page 211
- “IPv6 Neighbor Discovery Protocol” on page 226
- “IPv6 Routing” on page 232
- “IPv6 Tunnels” on page 233
- “IPv6 Extensions to Solaris Name Services” on page 241
- “NFS and RPC IPv6 Support” on page 244
- “IPv6 Over ATM Support” on page 244

For an overview of IPv6, refer to [Chapter 3](#). For tasks on configuring an IPv6-enabled network, refer to [Chapter 6](#).

IPv6 Addressing Formats Beyond the Basics

[Chapter 3](#) introduces the most common IPv6 addressing formats: unicast site address and link-local address. This section includes in-depth explanations of addressing formats that are not covered in detail in [Chapter 3](#):

- “6to4-Derived Addresses” on page 206
- “IPv6 Multicast Addresses in Depth” on page 207

6to4-Derived Addresses

If you plan to configure a 6to4 tunnel from a router or host endpoint, you must advertise the 6to4 site prefix in the `/etc/inet/ndpd.conf` file on the endpoint system. For an introduction and tasks for configuring 6to4 tunnels, refer to “How to Configure a 6to4 Tunnel” on page 133.

The next figure shows the parts of a 6to4 site prefix.

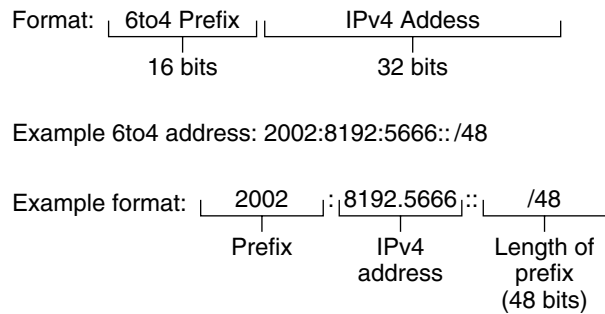


FIGURE 10-1 Parts of a 6to4 Site Prefix

The next figure shows the parts of a subnet prefix for a 6to4 site, such as you would include in the `ndpd.conf` file.

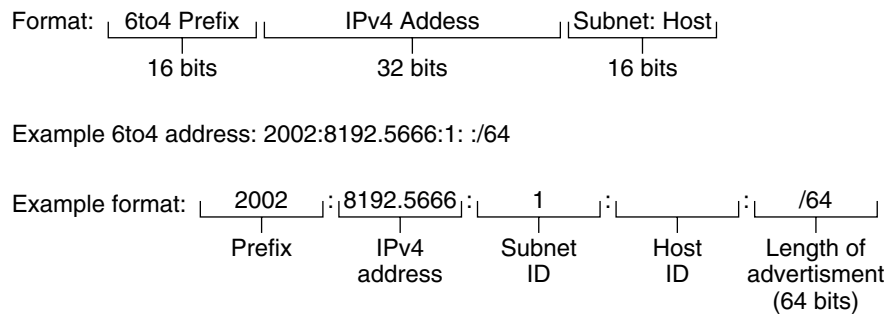


FIGURE 10-2 Parts of a 6to4 Subnet Prefix

This table explains the parts of a 6to4 subnet prefix.

Part	Length	Definition
Prefix	16 bits	6to4 prefix label 2002 (0x2002).

Part	Length	Definition
IPv4 address	32 bits	Unique IPv4 address that is already configured on the 6to4 interface. For the advertisement, you specify the hexadecimal representation of the IPv4 address, rather than the IPv4 dotted-decimal representation.
Subnet ID	16 bits	Subnet ID, which must be a value that is unique for the link at your 6to4 site.

6to4-Derived Addressing on a Host

When an IPv6 host receives the 6to4-derived prefix by way of a router advertisement, the host automatically reconfigures a 6to4-derived address on an interface. The address has the following format:

```
prefix:IPv4-address:subnet-ID:interface-ID/64
```

The output from the `ifconfig -a` command on a host with a 6to4 interface might resemble the following:

```
qfe1:3: flags=2180841<UP,RUNNING,MULTICAST,ADDRCONF,ROUTER,IPv6>
    mtu 1500 index 7
        inet6 2002:8192:56bb:9258:a00:20ff:fea9:4521/64
```

In this output, the 6to4-derived address follows `inet6`.

This table explains the parts of the 6to4-derived address.

Address Part	Length	Definition
<i>prefix</i>	16 bits	2002, which is the 6to4 prefix
<i>IPv4-address</i>	32 bits	8192:56bb, which is the IPv4 address, in hexadecimal notation, for the 6to4 pseudo-interface that is configured on the 6to4 router
<i>subnet-ID</i>	16 bits	9258, which is the address of the subnet of which this host is a member
<i>interface-ID</i>	64 bits	a00:20ff:fea9:4521, which is the interface ID of the host interface that is configured for 6to4

IPv6 Multicast Addresses in Depth

The IPv6 multicast address provides a method for distributing identical information or services to a defined group of interfaces, called the *multicast group*. Typically, the interfaces of the multicast group are on different nodes. An interface can belong to any

number of multicast groups. Packets sent to the multicast address go to all members of the multicast group. For example, one use of multicast addresses is for broadcasting information, similar to the capability of the IPv4 broadcast address.

The following table shows the format of the multicast address.

TABLE 10-1 IPv6 Multicast Address Format

8 bits	4 bits	4 bits	8 bits	8 bits	64 bits	32 bits
11111111	<i>FLGS</i>	SCOP	<i>Reserved</i>	<i>Plen</i>	<i>Network prefix</i>	<i>Group ID</i>

The following is a summary of the contents of each field.

- 11111111 – Identifies the address as a multicast address.
- *FLGS* – Set of the four flags 0,0,P,T. The first two flags must be zero. The P field has one of the following values:
 - 0 = Multicast address that is not assigned based on the network prefix
 - 1 = Multicast address that is assigned based on the network prefix

If P is set to 1, then T must also be 1.
- *Reserved* - Reserved value of zero.
- *Plen* - Number of bits in the site prefix that identify the subnet, for a multicast address that is assigned based on a site prefix.
- *Group ID* - Identifier for the multicast group, either permanent or dynamic.

For complete details about the multicast format, refer to RFC 3306, "Unicast-Prefix-based IPv6 Multicast Addresses" (<ftp://ftp.rfc-editor.org/in-notes/rfc3306.txt>).

Some IPv6 multicast addresses are permanently assigned by the Internet Assigned Numbers Authority (IANA). Some examples are the All Nodes Multicast Addresses and All Routers Multicast Addresses that are required by all IPv6 hosts and IPv6 routers. IPv6 multicast addresses can also be dynamically allocated. For more information about the proper use of multicast addresses and groups, see RFC 3307, "Allocation Guidelines for IPv6 Multicast Addresses".

IPv6 Packet Header Format

The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers. The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear.

Version	Traffic class	Flow label	
Payload length		Next header	Hop limit
Source address			
Destination address			

FIGURE 10-3 IPv6 Basic Header Format

The following list describes the function of each header field.

- **Version** – 4-bit version number of Internet Protocol = 6.
- **Traffic class** – 8-bit traffic class field.
- **Flow label** – 20-bit field.
- **Payload length** – 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets.
- **Next header** – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- **Hop limit** – 8-bit unsigned integer. Decrement by one by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero.
- **Source address** – 128 bits. The address of the initial sender of the packet.
- **Destination address** – 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is present.

IPv6 Extension Headers

IPv6 options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until the packet arrives at its final destination. This feature provides a major improvement in router performance for packets that contain options. In IPv4, the presence of any options requires the router to examine all options.

Unlike IPv4 options, IPv6 extension headers can be of arbitrary length. Also, the number of options that a packet carries is not limited to 40 bytes. This feature, in addition to the manner in which IPv6 options are processed, permits IPv6 options to be used for functions that are not practical in IPv4.

To improve performance when handling subsequent option headers, and the transport protocol that follows, IPv6 options are always an integer multiple of 8 octets long. The integer multiple of 8 octets retains the alignment of subsequent headers.

The following IPv6 extension headers are currently defined:

- **Routing** – Extended routing, such as IPv4 loose source route
- **Fragmentation** – Fragmentation and reassembly
- **Authentication** – Integrity and authentication, and security
- **Encapsulating Security Payload** – Confidentiality
- **Hop-by-Hop options** – Special options that require hop-by-hop processing
- **Destination options** – Optional information to be examined by the destination node

Dual-Stack Protocols

The term *dual-stack* normally refers to a complete duplication of all levels in the protocol stack from applications to the network layer. One example of complete duplication is a system that runs both the OSI and TCP/IP protocols.

The Solaris OS is *dual-stack*, meaning that the Solaris OS implements both IPv4 and IPv6 protocols. When you install the operating system, you can choose to enable the IPv6 protocols in the IP layer or use only the default IPv4 protocols. The remainder of the TCP/IP stack is identical. Consequently, the same transport protocols, TCP, UDP, and SCTP, can run over both IPv4 and IPv6. Also, the same applications can run over both IPv4 and IPv6. [Figure 10-4](#) shows how the IPv4 and IPv6 protocols work as a dual-stack throughout the various layers of the Internet protocol suite.

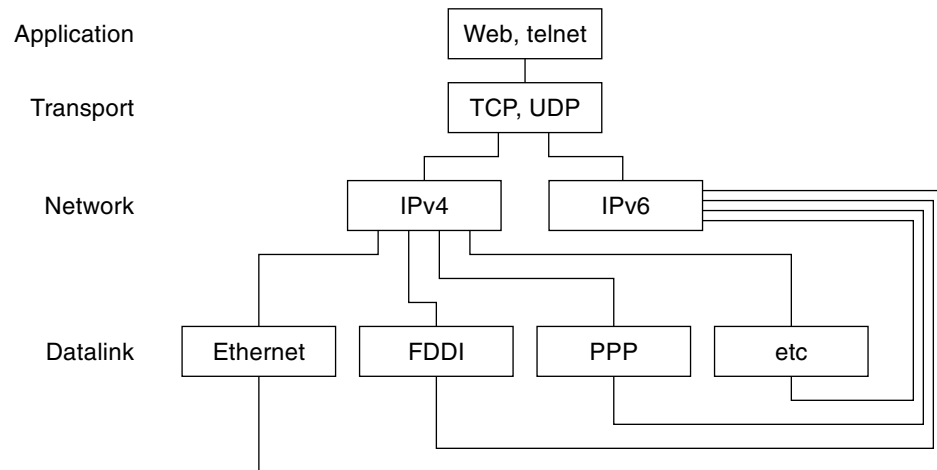


FIGURE 10-4 Dual-Stack Protocol Architecture

In the dual-stack scenario, subsets of both hosts and routers are upgraded to support IPv6, in addition to IPv4. The dual-stack approach ensures that the upgraded nodes can always interoperate with IPv4-only nodes by using IPv4.

Solaris 10 IPv6 Implementation

This section describes the files, commands, and daemons that enable IPv6 in the Solaris OS.

IPv6 Configuration Files

This section describes the configuration files that are part of an IPv6 implementation:

- [“ndpd.conf Configuration File” on page 211](#)
- [“IPv6 Interface Configuration File” on page 215](#)
- [“/etc/inet/ipaddrsel.conf Configuration File” on page 216](#)

ndpd.conf Configuration File

The `/etc/inet/ndpd.conf` file is used to configure options that are used by the `in.ndpd` Neighbor Discovery daemon. For a router, you primarily use `ndpd.conf` to configure the site prefix to be advertised to the link. For a host, you use `ndpd.conf` to turn off address autoconfiguration or to configure temporary addresses.

The next table shows the keywords that are used in the `ndpd.conf` file.

TABLE 10-2 `/etc/inet/ndpd.conf` Keywords

Variable	Description
<code>ifdefault</code>	Specifies the router behavior for all interfaces. Use the following syntax to set router parameters and corresponding values: <code>ifdefault [variable-value]</code>
<code>prefixdefault</code>	Specifies the default behavior for prefix advertisements. Use the following syntax to set router parameters and corresponding values: <code>prefixdefault [variable-value]</code>
<code>if</code>	Sets per-interface parameters. Use the following syntax: <code>if interface [variable-value]</code>
<code>prefix</code>	Advertises per-interface prefix information. Use the following syntax: <code>prefix prefix/length interface [variable-value]</code>

In the `ndpd.conf` file, you use the keywords in this table with a set of router configuration variables. These variables are defined in detail in RFC 2461, Neighbor Discovery for IP Version 6 (IPv6) (<http://www.ietf.org/rfc/rfc2461.txt?number=2461>).

The next table shows the variables for configuring an interface, along with brief definitions.

TABLE 10-3 `/etc/inet/ndpd.conf` Interface Configuration Variables

Variable	Default	Definition
<code>AdvRetransTimer</code>	0	Specifies the value in the Retrans Timer field in the advertisement messages sent by the router.
<code>AdvCurHopLimit</code>	Current diameter of the Internet	Specifies the value to be placed in the current hop limit in the advertisement messages sent by the router.
<code>AdvDefaultLifetime</code>	3 + <code>MaxRtrAdvInterval</code>	Specifies the default lifetime of the router advertisements.
<code>AdvLinkMTU</code>	0	Specifies a maximum transmission unit (MTU) value to be sent by the router. The zero indicates that the router does not specify MTU options.
<code>AdvManaged Flag</code>	False	Indicates the value to be placed in the Manage Address Configuration flag in the router advertisement.
<code>AdvOtherConfigFlag</code>	False	Indicates the value to be placed in the Other Stateful Configuration flag in the router advertisement.

TABLE 10-3 /etc/inet/ndpd.conf Interface Configuration Variables (Continued)

Variable	Default	Definition
AdvReachableTime	0	Specifies the value in the Reachable Time field in the advertisement messages sent by the router.
AdvSendAdvertisements	False	Indicates whether the node should send out advertisements and respond to router solicitations. You need to explicitly set this variable to "TRUE" in the ndpd.conf file to turn on router advertisement functions. For more information, refer to "How to Configure an IPv6-Enabled Router" on page 126.
DupAddrDetectTransmits	1	Defines the number of consecutive neighbor solicitation messages that the Neighbor Discovery protocol should send during duplicate address detection of the local node's address.
MaxRtrAdvInterval	600 seconds	Specifies the maximum time to wait between sending unsolicited multicast advertisements.
MinRtrAdvInterval	200 seconds	Specifies the minimum time to wait between sending unsolicited multicast advertisements.
StatelessAddrConf	True	Controls whether the node configures its IPv6 address through stateless address autoconfiguration. If False is declared in ndpd.conf, then the address must be manually configured. For more information, refer to "How to Manually Configure a Link-Local Address" on page 147.
TmpAdrsEnabled	False	Indicates whether a temporary address should be created for all interfaces or for a particular interface of a node. For more information, refer to "How to Configure a Temporary Address" on page 144.
TmpMaxDesyncFactor	600 seconds	Specifies a random value to be subtracted from the preferred lifetime variable TmpPreferredLifetime when in.ndpd starts. The purpose of the TmpMaxDesyncFactor variable is to prevent all the systems on your network from regenerating their temporary addresses at the same time. TmpMaxDesyncFactor allows you to change the upper bound on that random value.
TmpPreferredLifetime	False	Sets the preferred lifetime of a temporary address. For more information, refer to "How to Configure a Temporary Address" on page 144.
TmpRegenAdvance	False	Specifies the lead time in advance of address deprecation for a temporary address. For more information, refer to "How to Configure a Temporary Address" on page 144.

TABLE 10-3 /etc/inet/ndpd.conf Interface Configuration Variables (Continued)

Variable	Default	Definition
TmpValidLifetime	False	Sets the valid lifetime for a temporary address. For more information, refer to “How to Configure a Temporary Address” on page 144.

The next table shows the variables that are used for configuring IPv6 prefixes.

TABLE 10-4 /etc/inet/ndpd.conf Prefix Configuration Variables

Variable	Default	Definition
AdvAutonomousFlag	True	Specifies the value to be placed in the Autonomous Flag field in the Prefix Information option.
AdvOnLinkFlag	True	Specifies the value to be placed in the on-link flag (“L-bit”) in the Prefix Information option.
AdvPreferredExpiration	Not set	Specifies the preferred expiration date of the prefix.
AdvPreferredLifetime	604800 seconds	Specifies the value to be placed in the preferred lifetime in the Prefix Information option.
AdvValidExpiration	Not set	Specifies the valid expiration date of the prefix.
AdvValidLifetime	2592000 seconds	Specifies the valid lifetime of the prefix that is being configured.

EXAMPLE 10-1 /etc/inet/ndpd.conf File

The following example shows how the keywords and configuration variables are used in the ndpd.conf file. Remove the comment (#) to activate the variable.

```
# ifdefault      [variable-value ]*
# prefixdefault [variable-value ]*
# if ifname      [variable-value ]*
# prefix prefix/length ifname
#
# Per interface configuration variables
#
#DupAddrDetectTransmits
#AdvSendAdvertisements
#MaxRtrAdvInterval
#MinRtrAdvInterval
#AdvManagedFlag
#AdvOtherConfigFlag
#AdvLinkMTU
#AdvReachableTime
#AdvRetransTimer
#AdvCurHopLimit
#AdvDefaultLifetime
#
```

EXAMPLE 10-1 /etc/inet/ndpd.conf File (Continued)

```
# Per Prefix: AdvPrefixList configuration variables
#
#
#AdvValidLifetime
#AdvOnLinkFlag
#AdvPreferredLifetime
#AdvAutonomousFlag
#AdvValidExpiration
#AdvPreferredExpiration

ifdefault AdvReachableTime 30000 AdvRetransTimer 2000
prefixdefault AdvValidLifetime 240m AdvPreferredLifetime 120m

if qe0 AdvSendAdvertisements 1
prefix 2:0:0:56::/64 qe0
prefix fec0:0:0:56::/64 qe0

if qe1 AdvSendAdvertisements 1
prefix 2:0:0:55::/64 qe1
prefix fec0:0:0:56::/64 qe1

if hme1 AdvSendAdvertisements 1
prefix 2002:8192:56bb:1::/64 qfe0

if hme1 AdvSendAdvertisements 1
prefix 2002:8192:56bb:2::/64 hme1
```

IPv6 Interface Configuration File

IPv6 uses the `/etc/hostname6.interface` file at start up to automatically define IPv6 logical interfaces. When you select the IPv6 Enabled option during Solaris installation, the installation program creates an `/etc/hostname6.interface` file for the primary network interface, in addition to the `/etc/hostname.interface` file.

If more than one physical interface is detected during installation, you are prompted as to whether you want to configure these interfaces. The installation program creates IPv4 physical interface configuration files and IPv6 logical interface configuration files for each additional interface that you indicate.

As with IPv4 interfaces, you can also configure IPv6 interfaces manually, after Solaris installation. You create `/etc/hostname6.interface` files for the new interfaces. For instructions for manually configuring interfaces, refer to [“Administering Physical Interfaces” on page 112](#).

The network interface configuration file names have the following syntax:

```
hostname.interface
hostname6.interface
```

The `interface` variable has the following syntax:

dev [. *module* [. *module* . . .]] *PPA*

dev Indicates a network interface device. The device can be a physical network interface, such as *eri* or *qfe*, or a logical interface, such as a tunnel. See “IPv6 Interface Configuration File” on page 215 for more details.

Module Lists one or more STREAMS modules to be pushed onto the device when the device is plumbed.

PPA Indicates the physical point of attachment.

The syntax *[.|.]* is also accepted.

EXAMPLE 10–2 IPv6 Interface Configuration Files

The following are examples of valid IPv6 configuration file names:

```
hostname6.qfe0
hostname.ip.tun0
hostname.ip6.tun0
hostname6.ip6to4tun0
hostname6.ip.tun0
hostname6.ip6.tun0
```

/etc/inet/ipaddrsel.conf Configuration File

The `/etc/inet/ipaddrsel.conf` file contains the IPv6 default address selection policy table. When you install the Solaris OS with IPv6 enabled, this file contains the contents that are shown in Table 10–5.

You can edit the contents of `/etc/inet/ipaddrsel.conf`. However, in most cases, you should refrain from modifying this file. If modification is necessary, refer to the procedure “How to Administer the IPv6 Address Selection Policy Table” on page 174. For more information on `ipaddrsel.conf`, refer to “Reasons for Modifying the IPv6 Address Selection Policy Table” on page 217 and the `ipaddrsel.conf(4)` man page.

IPv6-Related Commands

This section describes commands that are added with the Solaris IPv6 implementation. The text also describes modifications to existing commands to support IPv6.

ipaddrsel Command

The `ipaddrsel` command enables you to modify the IPv6 default address selection policy table.

The Solaris kernel uses the IPv6 default address selection policy table to perform destination address ordering and source address selection for an IPv6 packet header. The `/etc/inet/ipaddrsel.conf` file contains the policy table.

The following table lists the default address formats and their priorities for the policy table. You can find technical details for IPv6 address selection in the `inet6(7P)` man page.

TABLE 10-5 IPv6 Address Selection Policy Table

Prefix	Precedence	Definition
::1/128	50	Loopback
::/0	40	Default
2002::/16	30	6to4
::/96	20	IPv4 Compatible
::ffff:0:0/96	10	IPv4

In this table, IPv6 prefixes (::1/128 and ::/0) take precedence over 6to4 addresses (2002::/16) and IPv4 addresses (::/96 and ::ffff:0:0/96). Therefore, by default, the kernel selects the global IPv6 address of the interface for packets going to another IPv6 destination. The IPv4 address of the interface has a lower priority, particularly for packets going to an IPv6 destination. Given the selected IPv6 source address, the kernel also uses the IPv6 format for the destination address.

Reasons for Modifying the IPv6 Address Selection Policy Table

Under most instances, you do not need to change the IPv6 default address selection policy table. If you do need to administer the policy table, you use the `ipaddrsel` command.

You might want to modify the policy table under the following circumstances:

- If the system has an interface that is used for a 6to4 tunnel, you can give higher priority to 6to4 addresses.
- If you want a particular source address to be used only in communications with a particular destination address, you can add these addresses to the policy table. Then, you can use `ifconfig` to flag these addresses as preferred.
- If you want IPv4 addresses to take precedence over IPv6 addresses, you can change the priority of ::ffff:0:0/96 to a higher number.
- If you need to assign a higher priority to deprecated addresses, you can add the deprecated address to the policy table. For example, site-local addresses are now deprecated in IPv6. These addresses have the prefix `fec0::/10`. You can change the policy table to give higher priority to site-local addresses.

For details about the `ipaddrsel` command, refer to the `ipaddrsel(1M)` man page.

6to4relay Command

6to4 tunneling enables communication between isolated 6to4 sites. However, to transfer packets with a native, non-6to4 IPv6 site, the 6to4 router must establish a tunnel with a 6to4 relay router. The *6to4 relay router* then forwards the 6to4 packets to the IPv6 network and ultimately, to the native IPv6 site. If your 6to4-enabled site must exchange data with a native IPv6 site, you use the `6to4relay` command to enable the appropriate tunnel.

Because the use of relay routers is insecure, tunneling to a relay router is disabled by default in the Solaris OS. Carefully consider the issues that are involved in creating a tunnel to a 6to4 relay router before deploying this scenario. For detailed information on 6to4 relay routers, refer to [“Considerations for Tunnels to a 6to4 Relay Router” on page 239](#). If you decide to enable 6to4 relay router support, you can find the related procedures in [“How to Configure a 6to4 Tunnel” on page 133](#).

Syntax of 6to4relay

The `6to4relay` command has the following syntax:

```
6to4relay -e [-a IPv4-address] -d -h
```

<code>-e</code>	Enables support for tunnels between the 6to4 router and an anycast 6to4 relay router. The tunnel endpoint address is then set to <code>192.88.99.1</code> , the default address for the anycast group of 6to4 relay routers.
<code>-a IPv4-address</code>	Enables support for tunnels between the 6to4 router and a 6to4 relay router with the specified <i>IPv4-address</i> .
<code>-d</code>	Disables support for tunneling to the 6to4 relay router, the default for the Solaris OS.
<code>-h</code>	Displays help for <code>6to4relay</code> .

For more information, refer to the `6to4relay(1M)` man page.

EXAMPLE 10-3 Default Status Display of 6to4 Relay Router Support

The `6to4relay` command, without arguments, shows the current status of 6to4 relay router support. This example shows the default for the Solaris OS implementation of IPv6.

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is disabled
```

EXAMPLE 10-4 Status Display With 6to4 Relay Router Support Enabled

If relay router support is enabled, `6to4relay` displays the following output:

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is enabled
```

EXAMPLE 10-4 Status Display With 6to4 Relay Router Support Enabled (Continued)

```
IPv4 destination address of Relay Router=192.88.99.1
```

EXAMPLE 10-5 Status Display With a 6to4 Relay Router Specified

If you specify the `-a` option and an IPv4 address to the `6to4relay` command, the IPv4 address that you give with `-a` is displayed instead of `192.88.99.1`.

`6to4relay` does not report successful execution of the `-d`, `-e`, and `-a IPv4 address` options. However, `6to4relay` does display any error messages that might be generated when you run these options.

`ifconfig` Command Extensions for IPv6 Support

The `ifconfig` command enables IPv6 interfaces and the tunneling module to be plumbed. `ifconfig` uses an extended set of ioctls to configure both IPv4 and IPv6 network interfaces. The following describes `ifconfig` options that support IPv6 operations. See “[Monitoring the Interface Configuration With the `ifconfig` Command](#)” on page 153 for a range of both IPv4 and IPv6 tasks that involve `ifconfig`.

<code>index</code>	Sets the interface index.
<code>tsrc/tdst</code>	Sets the tunnel source or destination.
<code>addif</code>	Creates the next available logical interface.
<code>removeif</code>	Deletes a logical interface with a specific IP address.
<code>destination</code>	Sets the point-to-point destination address for an interface.
<code>set</code>	Sets an address, netmask, or both for an interface.
<code>subnet</code>	Sets the subnet address of an interface.
<code>xmit/-xmit</code>	Enables or disables packet transmission on an interface.

[Chapter 6](#) provides IPv6 configuration procedures.

EXAMPLE 10-6 Adding a Logical IPv6 Interface With the `-addif` Option of the `ifconfig` Command

The following form of the `ifconfig` command creates the `hme0:3` logical interface:

```
# ifconfig hme0 inet6 addif up
Created new logical interface hme0:3
```

This form of `ifconfig` verifies the creation of the new interface:

EXAMPLE 10-6 Adding a Logical IPv6 Interface With the `-addif` Option of the `ifconfig` Command (Continued)

```
# ifconfig hme0:3 inet6
hme0:3: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        inet6 inet6 fe80::203:baff:fe11:b321/10
```

EXAMPLE 10-7 Removing a Logical IPv6 Interface With the `-removeif` Option of the `ifconfig` Command

The following form of the `ifconfig` command removes the `hme0:3` logical interface.

```
# ifconfig hme0:3 inet6 down
# ifconfig hme0 inet6 removeif 1234::5678
```

EXAMPLE 10-8 Using `ifconfig` to Configure an IPv6 Tunnel Source

```
# ifconfig ip.tun0 inet6 plumb index 13
```

Opens the tunnel to be associated with the physical interface name.

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NUD,
#IPv6> mtu 1480 index 13
        inet tunnel src 0.0.0.0
        inet6 fe80::/10 --> ::
```

Configures the streams that are needed for TCP/IP to use the tunnel device and report the status of the device.

```
# ifconfig ip.tun0 inet6 tsrc 120.46.86.158 tdst 120.46.86.122
```

Configures the source and the destination address for the tunnel.

```
# ifconfig ip.tun0 inet6
ip.tun0: flags=2200850<POINTOPOINT,RUNNING,MULTICAST,NUD,
IPv6> mtu 1480 index 13
        inet tunnel src 120.46.86.158 tunnel dst 120.46.86.122
        inet6 fe80::8192:569e/10 --> fe80::8192:567a
```

Reports the new status of the device after the configuration.

EXAMPLE 10-9 Configuring a 6to4 Tunnel Through `ifconfig` (Long Form)

This example of a 6to4 pseudo-interface configuration uses the subnet ID of 1 and specifies the host ID, in hexadecimal form.

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 \
2002:8192:56bb:1::8192:56bb/64 up
```

EXAMPLE 10-9 Configuring a 6to4 Tunnel Through `ifconfig` (Long Form) *(Continued)*

```
# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NUD,IPv6>mtu 1480 index 11
    inet tunnel src 129.146.86.187
    tunnel hop limit 60
    inet6 2002:8192:56bb:1::8192:56bb/64
```

EXAMPLE 10-10 Configuring a 6to4 Tunnel Through `ifconfig` (Short Form)

This example shows the short form for configuring a 6to4 tunnel.

```
# ifconfig ip.6to4tun0 inet6 plumb
# ifconfig ip.6to4tun0 inet tsrc 129.146.86.187 up

# ifconfig ip.6to4tun0 inet6
ip.6to4tun0: flags=2200041<UP,RUNNING,NUD,IPv6>mtu 1480 index 11
    inet tunnel src 129.146.86.187
    tunnel hop limit 60
    inet6 2002:8192:56bb::1/64
```

netstat Command Modifications for IPv6 Support

The `netstat` command displays both IPv4 and IPv6 network status. You can choose which protocol information to display by setting the `DEFAULT_IP` value in the `/etc/default/inet_type` file or by using the `-f` command-line option. With a permanent setting of `DEFAULT_IP`, you can ensure that `netstat` displays only IPv4 information. You can override this setting by using the `-f` option. For more information on the `inet_type` file, see the `inet_type(4)` man page.

The `-p` option of the `netstat` command displays the net-to-media table, which is the ARP table for IPv4 and the neighbor cache for IPv6. See the `netstat(1M)` man page for details. See [“How to Display the Status of Sockets” on page 160](#) for descriptions of procedures that use this command.

snoop Command Modifications for IPv6 Support

The `snoop` command can capture both IPv4 and IPv6 packets. This command can display IPv6 headers, IPv6 extension headers, ICMPv6 headers, and Neighbor Discovery protocol data. By default, the `snoop` command displays both IPv4 and IPv6 packets. If you specify the `ip` or `ip6` protocol keyword, the `snoop` command displays only IPv4 or IPv6 packets. The IPv6 filter option enables you to filter through all packets, both IPv4 and IPv6, displaying only the IPv6 packets. See the `snoop(1M)` man page for details. See [“How to Monitor IPv6 Network Traffic” on page 173](#) for procedures that use the `snoop` command.

route Command Modifications for IPv6 Support

The `route` command operates on both IPv4 and IPv6 routes, with IPv4 routes as the default. If you use the `-inet6` option on the command line immediately after the `route` command, operations are performed on IPv6 routes. See the `route(1M)` man page for details.

ping Command Modifications for IPv6 Support

The `ping` command can use both IPv4 and IPv6 protocols to probe target hosts. Protocol selection depends on the addresses that are returned by the name server for the specific target host. By default, if the name server returns an IPv6 address for the target host, the `ping` command uses the IPv6 protocol. If the server returns only an IPv4 address, the `ping` command uses the IPv4 protocol. You can override this action by using the `-A` command-line option to specify which protocol to use.

For detailed information, see the `ping(1M)` man page. For procedures that use `ping`, refer to [“Probing Remote Hosts With the ping Command” on page 164](#).

traceroute Command Modifications for IPv6 Support

You can use the `traceroute` command to trace both the IPv4 and IPv6 routes to a specific host. From a protocol perspective, `traceroute` uses the same algorithm as `ping`. Use the `-A` command-line option to override this selection. You can trace each individual route to every address of a multihomed host by using the `-a` command-line option.

For detailed information, see the `traceroute(1M)` man page. For procedures that use `traceroute`, refer to [“Displaying Routing Information With the traceroute Command” on page 168](#).

IPv6-Related Daemons

This section discusses the IPv6-related daemons.

`in.ndpd` Daemon, for Neighbor Discovery

The `in.ndpd` daemon implements the IPv6 Neighbor Discovery protocol and router discovery. The daemon also implements address autoconfiguration for IPv6. The following shows the supported options of `in.ndpd`.

`-d` Turns on debugging.

- D Turns on debugging for specific events.
- f Specifies a file to read configuration data from, instead of the default `/etc/inet/ndpd.conf` file.
- I Prints related information for each interface.
- n Does not loop back router advertisements.
- r Ignores received packets.
- v Specifies verbose mode, reporting various types of diagnostic messages.
- t Turns on packet tracing.

The `in.ndpd` daemon is controlled by parameters that are set in the `/etc/inet/ndpd.conf` configuration file and any applicable parameters in the `/var/inet/ndpd_state.interface` startup file.

When the `/etc/inet/ndpd.conf` file exists, the file is parsed and used to configure a node as a router. Table 10–2 lists the valid keywords that might appear in this file. When a host is booted, routers might not be immediately available. Advertised packets by the router might be dropped. Also, advertised packets might not reach the host.

The `/var/inet/ndpd_state.interface` file is a state file. This file is updated periodically by each node. When the node fails and is restarted, the node can configure its interfaces in the absence of routers. This file contains the interface address, the last time that the file was updated, and how long the file is valid. This file also contains other parameters that are “learned” from previous router advertisements.

Note – You do not need to alter the contents of state files. The `in.ndpd` daemon automatically maintains state files.

See the `in.ndpd(1M)` man page and the `ndpd.conf(4)` man page for lists of configuration variables and allowable values.

`in.ripngd` Daemon, for IPv6 Routing

The `in.ripngd` daemon implements the Routing Information Protocol next-generation for IPv6 routers (RIPng). RIPng defines the IPv6 equivalent of RIP. When you configure an IPv6 router with the `routeadm` command and turn on IPv6 routing, the `in.ripngd` daemon implements RIPng on the router.

The following shows the supported options of RIPng.

- p *n* *n* specifies the alternate port number that is used to send or receive RIPnG packets.
- q Suppresses routing information.
- s Forces routing information even if the daemon is acting as a router.
- P Suppresses use of poison reverse.
- S If `in.ripngd` does not act as a router, the daemon enters only a default route for each router.

inetd Daemon and IPv6 Services

An IPv6-enabled server application can handle both IPv4 requests and IPv6 requests, or IPv6 requests only. The server always handles requests through an IPv6 socket. Additionally, the server uses the same protocol that the corresponding client uses. To add or modify a service for IPv6, use the commands available from the Service Management Facility (SMF).

- For information about the SMF commands, refer to “SMF Command-Line Administrative Utilities” in *System Administration Guide: Basic Administration*.
- For an example task that uses SMF to configure an IPv4 service manifest that runs over SCTP, refer to “How to Add Services That Use the SCTP Protocol” on page 109.

To configure an IPv6 service, you must ensure that the `proto` field value in the `inetadm` profile for that service lists the appropriate value:

- For a service that handles both IPv4 and IPv6 requests, choose `tcp6`, `udp6`, or `sctp`. A `proto` value of `tcp6`, `udp6`, or `sctp6` causes `inetd` to pass on an IPv6 socket to the server. The server contains an IPv4-mapped address in case a IPv4 client has a request.
- For a service that handles only IPv6 requests, choose `tcp6only` or `udp6only`. With either of these values for `proto`, `inetd` passes the server an IPv6 socket.

If you replace a Solaris command with another implementation, you must verify that the implementation of that service supports IPv6. If the implementation does not support IPv6, then you must specify the `proto` value as either `tcp`, `udp`, or `sctp`.

Here is a profile that results from running `inetadm` for an `echo` service manifest that supports both IPv4 and IPv6 and runs over SCTP:

```
# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE      name="echo"
            endpoint_type="stream"
            proto="sctp6"
            isrpc=FALSE
            wait=FALSE
            exec="/usr/lib/inet/in.echod -s"
```



```

        user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=FALSE
default  tcp_wrappers=FALSE

```

To change the value of the `proto` field, use the following syntax:

```
# inetadm -m EMRI proto="transport-protocols"
```

All servers that are provided with Solaris software require only one profile entry that specifies `proto` as `tcp6`, `udp6`, or `sctp6`. However, the remote shell server (`shell`) and the remote execution server (`exec`) now are composed of a single service instance, which requires a `proto` value containing both the `tcp` and `tcp6only` values. For example, to set the `proto` value for `shell`, you would issue the following command:

```
# inetadm -m network/shell:default proto="tcp,tcp6only"
```

See IPv6 extensions to the Socket API in *Programming Interfaces Guide* for more details on writing IPv6-enabled servers that use sockets.

Considerations When Configuring a Service for IPv6

When you add or modify a service for IPv6, keep in mind the following caveats:

- You need to specify the `proto` value as `tcp6`, `sctp6`, or `udp6` to enable both IPv4 or IPv6 connections. If you specify the value for `proto` as `tcp`, `sctp`, or `udp`, the service uses only IPv4.
- Though you can add a service instance that uses one-to-many style SCTP sockets for `inetd`, this is not recommended. `inetd` does not work with one-to-many style SCTP sockets.
- If a service requires two entries because its `wait-status` or `exec` properties differ, then you must create two instances/services from the original service.

IPv6 Neighbor Discovery Protocol

IPv6 introduces the Neighbor Discovery protocol, as described in RFC 2461, Neighbor Discovery for IP Version 6 (IPv6)

(<http://www.ietf.org/rfc/rfc2461.txt?number=2461>). For an overview of major Neighbor Discovery features, refer to “IPv6 Neighbor Discovery Protocol Overview” on page 81.

This section discusses the following features of the Neighbor Discovery protocol:

- “ICMP Messages From Neighbor Discovery” on page 226
- “Autoconfiguration Process” on page 227
- “Neighbor Solicitation and Unreachability” on page 229
- “Duplicate Address Detection Algorithm” on page 229
- “Comparison of Neighbor Discovery to ARP and Related IPv4 Protocols” on page 230

ICMP Messages From Neighbor Discovery

Neighbor Discovery defines five new Internet Control Message Protocol (ICMP) messages. The messages serve the following purposes:

- **Router solicitation** – When an interface becomes enabled, hosts can send router solicitation messages. The solicitations request routers to generate router advertisements immediately, rather than at their next scheduled time.
- **Router advertisement** – Routers advertise their presence, various link parameters, and various Internet parameters. Routers advertise either periodically, or in response to a router solicitation message. Router advertisements contain prefixes that are used for on-link determination or address configuration, a suggested hop-limit value, and so on.
- **Neighbor solicitation** – Nodes send neighbor solicitation messages to determine the link-layer address of a neighbor. Neighbor solicitation messages are also sent to verify that a neighbor is still reachable by a cached link-layer address. Neighbor solicitations are also used for duplicate address detection.
- **Neighbor advertisement** – A node sends neighbor advertisement messages in response to a neighbor solicitation message. The node can also send unsolicited neighbor advertisements to announce a link-layer address change.
- **Redirect** – Routers use redirect messages to inform hosts of a better first hop for a destination, or that the destination is on the same link.

Autoconfiguration Process

This section provides an overview of the typical steps that are performed by an interface during autoconfiguration. Autoconfiguration is performed only on multicast-capable links.

1. A multicast-capable interface is enabled, for example, during system startup of a node.
2. The node begins the autoconfiguration process by generating a link-local address for the interface.

The link-local address is formed from the Media Access Control (MAC) address of the interface.

3. The node sends a neighbor solicitation message that contains the tentative link-local address as the target.

The purpose of the message is to verify that the prospective address is not already in use by another node on the link. After verification, the link-local address can be assigned to an interface.

- a. If another node already uses the proposed address, that node returns a neighbor advertisement stating that the address is already in use.
- b. If another node is also attempting to use the same address, the node also sends a neighbor solicitation for the target.

The number of neighbor solicitation transmissions or retransmissions, and the delay between consecutive solicitations, are link specific. You can set these parameters, if necessary.

4. If a node determines that its prospective link-local address is not unique, autoconfiguration stops. At that point, you must manually configure the link-local address of the interface.

To simplify recovery, you can supply an alternate interface ID that overrides the default identifier. Then, the autoconfiguration mechanism can resume by using the new, presumably unique, interface ID.

5. When a node determines that its prospective link-local address is unique, the node assigns the address to the interface.

At this point, the node has IP-level connectivity with neighboring nodes. The remaining autoconfiguration steps are performed only by hosts.

Obtaining a Router Advertisement

The next phase of autoconfiguration involves obtaining a router advertisement or determining that no routers are present. If routers are present, the routers send router advertisements that specify what type of autoconfiguration a host should perform.

Routers send router advertisements periodically. However, the delay between successive advertisements is generally longer than a host that performs autoconfiguration can wait. To quickly obtain an advertisement, a host sends one or more router solicitations to the all-routers multicast group.

Prefix Configuration Variables

Router advertisements also contain prefix variables with information that stateless address autoconfiguration uses to generate prefixes. The Stateless Address Autoconfiguration field in router advertisements are processed independently. One option field that contains prefix information, the Address Autoconfiguration flag, indicates whether the option even applies to stateless autoconfiguration. If the option field does apply, additional option fields contain a subnet prefix with lifetime values. These values indicate the length of time that addresses created from the prefix remain preferred and valid.

Because routers periodically generate router advertisements, hosts continually receive new advertisements. IPv6-enabled hosts process the information that is contained in each advertisement. Hosts add to the information. They also refresh the information that is received in previous advertisements.

Address Uniqueness

For security reasons, all addresses must be tested for uniqueness prior to their assignment to an interface. The situation is different for addresses that are created through stateless autoconfiguration. The uniqueness of an address is determined primarily by the portion of the address that is formed from an interface ID. Thus, if a node has already verified the uniqueness of a link-local address, additional addresses need not be tested individually. The addresses must be created from the same interface ID. In contrast, all addresses that are obtained manually should be tested individually for uniqueness. System administrators at some sites believe that the overhead of performing duplicate address detection outweighs its benefits. For these sites, the use of duplicate address detection can be disabled by setting a per-interface configuration flag.

To accelerate the autoconfiguration process, a host can generate its link-local address, and verify its uniqueness, while the host waits for a router advertisement. A router might delay a response to a router solicitation for a few seconds. Consequently, the total time necessary to complete autoconfiguration can be significantly longer if the two steps are done serially.

Neighbor Solicitation and Unreachability

Neighbor Discovery uses *neighbor solicitation* messages to determine if more than one node is assigned the same unicast address. *Neighbor unreachability detection* detects the failure of a neighbor or the failure of the forward path to the neighbor. This detection requires positive confirmation that packets that are sent to a neighbor are actually reaching that neighbor. Neighbor unreachability detection also determines that packets are being processed properly by the node's IP layer.

Neighbor unreachability detection uses confirmation from two sources: upper-layer protocols and neighbor solicitation messages. When possible, upper-layer protocols provide a positive confirmation that a connection is making *forward progress*. For example, when new TCP acknowledgments are received, it is confirmed that previously sent data has been delivered correctly.

When a node does not get positive confirmation from upper-layer protocols, the node sends unicast neighbor solicitation messages. These messages solicit neighbor advertisements as reachability confirmation from the next hop. To reduce unnecessary network traffic, probe messages are sent only to neighbors to which the node is actively sending packets.

Duplicate Address Detection Algorithm

To ensure that all configured addresses are likely to be unique on a particular link, nodes run a *duplicate address detection* algorithm on addresses. The nodes must run the algorithm before assigning the addresses to an interface. The duplicate address detection algorithm is performed on all addresses.

The autoconfiguration process that is described in this section applies only to hosts, and not routers. Because host autoconfiguration uses information that is advertised by routers, routers need to be configured by some other means. However, routers generate link-local addresses by using the mechanism that is described in this chapter. In addition, routers are expected to successfully pass the duplicate address detection algorithm on all addresses prior to assigning the address to an interface.

Proxy Advertisements

A router that accepts packets on behalf of a target address can issue non-override neighbor advertisements. The router can accept packets for a target address that is unable to respond to neighbor solicitations. Currently, the use of proxy is not specified. However, proxy advertising can potentially be used to handle cases such as mobile nodes that have moved off-link. Note that the use of proxy is not intended as a general mechanism to handle nodes that do not implement this protocol.

Inbound Load Balancing

Nodes with replicated interfaces might need to load balance the reception of incoming packets across multiple network interfaces on the same link. Such nodes have multiple link-local addresses assigned to the same interface. For example, a single network driver can represent multiple network interface cards as a single logical interface that has multiple link-local addresses.

Load balancing is handled by allowing routers to omit the source link-local address from router advertisement packets. Consequently, neighbors must use neighbor solicitation messages to learn link-local addresses of routers. Returned neighbor advertisement messages can then contain link-local addresses that differ, depending on which issued the solicitation.

Link-Local Address Change

A node that knows its link-local address has been changed can send out multicast unsolicited, neighbor advertisement packets. The node can send multicast packets to all nodes to update cached link-local addresses that have become invalid. The sending of unsolicited advertisements is a performance enhancement only. The detection algorithm for neighbor unreachability ensures that all nodes reliably discover the new address, though the delay might be somewhat longer.

Comparison of Neighbor Discovery to ARP and Related IPv4 Protocols

The functionality of the IPv6 Neighbor Discovery protocol corresponds to a combination of the IPv4 protocols: Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery, and ICMP Redirect. IPv4 does not have a generally agreed on protocol or mechanism for neighbor unreachability detection. However, host requirements do specify some possible algorithms for dead gateway detection. Dead gateway detection is a subset of the problems that neighbor unreachability detection solves.

The following list compares the Neighbor Discovery protocol to the related set of IPv4 protocols.

- Router discovery is part of the base IPv6 protocol set. IPv6 hosts do not need to snoop the routing protocols to find a router. IPv4 uses ARP, ICMP router discovery, and ICMP redirect for router discovery.
- IPv6 router advertisements carry link-local addresses. No additional packet exchange is needed to resolve the router's link-local address.

- Router advertisements carry site prefixes for a link. A separate mechanism is not needed to configure the netmask, as is the case with IPv4.
- Router advertisements enable address autoconfiguration. Autoconfiguration is not implemented in IPv4.
- Neighbor Discovery enables IPv6 routers to advertise an MTU for hosts to use on the link. Consequently, all nodes use the same MTU value on links that lack a well-defined MTU. IPv4 hosts on the same network might have different MTUs.
- Unlike IPv4 broadcast addresses, IPv6 address resolution multicasts are spread over 4 billion (2^{32}) multicast addresses, greatly reducing address resolution-related interrupts on nodes other than the target. Moreover, non-IPv6 machines should not be interrupted at all.
- IPv6 redirects contain the link-local address of the new first hop. Separate address resolution is not needed on receiving a redirect.
- Multiple site prefixes can be associated with the same IPv6 network. By default, hosts learn all local site prefixes from router advertisements. However, routers can be configured to omit some or all prefixes from router advertisements. In such instances, hosts assume that destinations are on remote networks. Consequently, hosts send the traffic to routers. A router can then issue redirects, as appropriate.
- Unlike IPv4, the recipient of an IPv6 redirect message assumes that the new next-hop is on the local network. In IPv4, a host ignores redirect messages that specify a next-hop that is not on the local network, according to the network mask. The IPv6 redirect mechanism is analogous to the XRedirect facility in IPv4. The redirect mechanism is useful on non-broadcast and shared media links. On these networks, nodes should not check for all prefixes for local link destinations.
- IPv6 neighbor unreachability detection improves packet delivery in the presence of failing routers. This capability improves packet delivery over partially failing or partitioned links. This capability also improves packet delivery over nodes that change their link-local addresses. For example, mobile nodes can move off the local network without losing any connectivity because of stale ARP caches. IPv4 has no corresponding method for neighbor unreachability detection.
- Unlike ARP, Neighbor Discovery detects half-link failures by using neighbor unreachability detection. Neighbor Discovery avoids sending traffic to neighbors when two-way connectivity is absent.
- By using link-local addresses to uniquely identify routers, IPv6 hosts can maintain the router associations. The ability to identify routers is required for router advertisements and for redirect messages. Hosts need to maintain router associations if the site uses new global prefixes. IPv4 does not have a comparable method for identifying routers.
- Because Neighbor Discovery messages have a hop limit of 255 upon receipt, the protocol is immune to spoofing attacks originating from off-link nodes. In contrast, IPv4 off-link nodes can send ICMP redirect messages. IPv4 off-link nodes can also send router advertisement messages.

- By placing address resolution at the ICMP layer, Neighbor Discovery becomes more media independent than ARP. Consequently, standard IP authentication and security mechanisms can be used.

IPv6 Routing

Routing in IPv6 is almost identical to IPv4 routing under Classless Inter-Domain Routing (CIDR). The only difference is that the addresses are 128-bit IPv6 addresses instead of 32-bit IPv4 addresses. With very straightforward extensions, all of IPv4's routing algorithms, such as OSPF, RIP, IDRP, and IS-IS, can be used to route IPv6.

IPv6 also includes simple routing extensions that support powerful new routing capabilities. The following list describes the new routing capabilities:

- Provider selection that is based on policy, performance, cost, and so on
- Host mobility, route to current location
- Auto-readdressing, route to new address

You obtain the new routing capabilities by creating sequences of IPv6 addresses that use the IPv6 routing option. An IPv6 source uses the routing option to list one or more intermediate nodes, or topological group, to be visited on the way to a packet's destination. This function is very similar in function to IPv4's loose source and record route option.

To make address sequences a general function, IPv6 hosts are required, in most instances, to reverse routes in a packet that a host receives. The packet must be successfully authenticated by using the IPv6 authentication header. The packet must contain address sequences in order to return the packet to its originator. This technique forces IPv6 host implementations to support the handling and reversal of source routes. The handling and reversal of source routes is the key that enables providers to work with hosts that implement the new IPv6 capabilities such as provider selection and extended addresses.

Router Advertisement

On multicast-capable links and point-to-point links, each router periodically sends to the multicast group a router advertisement packet that announces its availability. A host receives router advertisements from all routers, building a list of default routers. Routers generate router advertisements frequently enough so that hosts learn of their presence within a few minutes. However, routers do not advertise frequently enough to rely on an absence of advertisements to detect router failure. A separate detection algorithm that determines neighbor unreachability provides failure detection.

Router Advertisement Prefixes

Router advertisements contain a list of subnet prefixes that is used to determine if a host is on the same link (on-link) as the router. The list of prefixes is also used for autonomous address configuration. Flags that are associated with the prefixes specify the intended uses of a particular prefix. Hosts use the advertised on-link prefixes to build and maintain a list that is used to decide when a packet's destination is on-link or beyond a router. A destination can be on-link even though the destination is not covered by any advertised on-link prefix. In such instances, a router can send a redirect. The redirect informs the sender that the destination is a neighbor.

Router advertisements, and per-prefix flags, enable routers to inform hosts how to perform stateless address autoconfiguration.

Router Advertisement Messages

Router advertisement messages also contain Internet parameters, such as the hop limit, that hosts should use in outgoing packets. Optionally, router advertisement messages also contain link parameters, such as the link MTU. This feature enables the centralized administration of critical parameters. The parameters can be set on routers and automatically propagated to all hosts that are attached.

Nodes accomplish address resolution by sending to the multicast group a neighbor solicitation that asks the target node to return its link-layer address. Multicast neighbor solicitation messages are sent to the solicited-node multicast address of the target address. The target returns its link-layer address in a unicast neighbor advertisement message. A single request-response pair of packets is sufficient for both the initiator and the target to resolve each other's link-layer addresses. The initiator includes its link-layer address in the neighbor solicitation.

IPv6 Tunnels

To minimize any dependencies at a dual-stack, IPv4/IPv6 site, all the routers in the path between two IPv6 nodes do not need to support IPv6. The mechanism that supports such a network configuration is called *tunneling*. Basically, IPv6 packets are placed inside IPv4 packets, which are then routed through the IPv4 routers. The following figure illustrates the tunneling mechanism through IPv4 routers, which are indicated in the figure by "R."

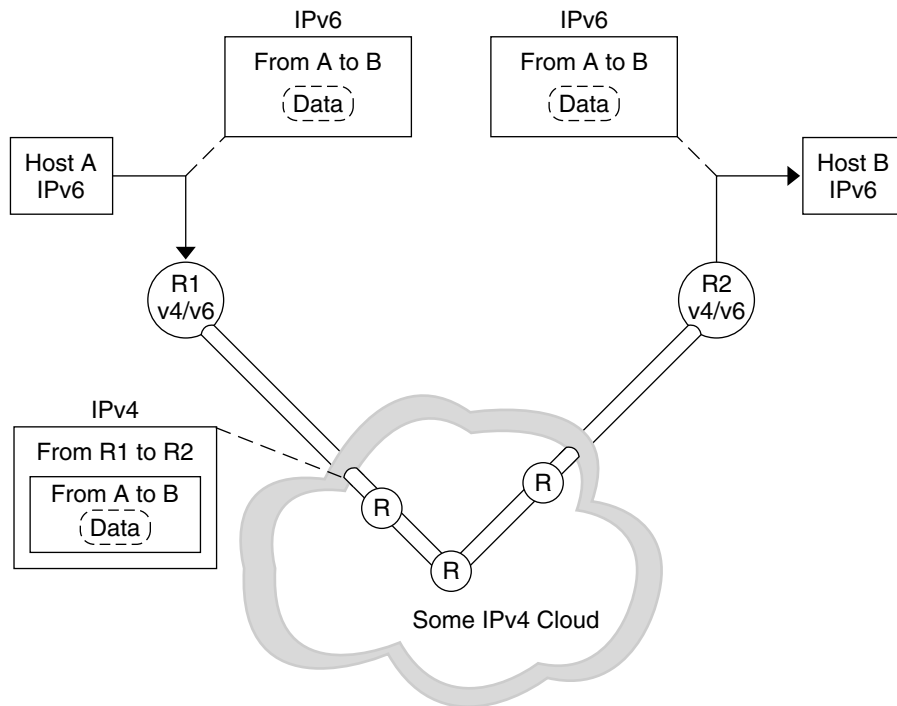


FIGURE 10-5 IPv6 Tunneling Mechanism

The Solaris IPv6 implementation includes two types of tunneling mechanisms:

- Configured tunnels between two routers, as in [Figure 10-5](#)
- Automatic tunnels that terminate at the endpoint hosts

A configured tunnel is currently used on the Internet for other purposes, for example, on the MBONE, the IPv4 multicast backbone. Operationally, the tunnel consists of two routers that are configured to have a virtual point-to-point link between the two routers over the IPv4 network. This kind of tunnel is likely to be used on some parts of the Internet for the foreseeable future.

Automatic tunnels require IPv4-compatible addresses. Automatic tunnels can be used to connect IPv6 nodes when IPv6 routers are not available. These tunnels can originate either on a dual-stack host or on a dual-stack router by configuring an automatic tunneling network interface. The tunnels always terminate on the dual-stack host. These tunnels work by dynamically determining the destination IPv4 address, which is the endpoint of the tunnel, by extracting the address from the IPv4-compatible destination address.

Configured Tunnels

Tunneling interfaces have the following format:

```
ip.tun ppa
```

ppa is the physical point of attachment.

At system startup, the tunneling module (`tun`) is pushed, by the `ifconfig` command, on top of IP to create a virtual interface. The push is accomplished by creating the appropriate `hostname6.*` file.

For example, to create a tunnel to encapsulate IPv6 packets over an IPv4 network, IPv6 over IPv4, you would create the following file name:

```
/etc/hostname6.ip.tun0
```

The content of this file is passed to `ifconfig` after the interfaces have been plumbed. The content becomes the parameters that are necessary to configure a point-to-point tunnel.

EXAMPLE 10–11 `hostname6.ip.tun0` File for an IPv6 Over IPv4 Tunnel

The following is an example of entries in the `hostname6.ip.tun0` file:

```
tsrc 10.10.10.23 tdst 172.16.7.19 up
addif 2001:db8:3b4c:1:5678:5678::2 up
```

In this example, the IPv4 source and destination addresses are used as tokens to autoconfigure IPv6 link-local addresses. These addresses are the source and destination for the `ip.tun0` interface. Two interfaces are configured. The `ip.tun0` interface is configured. A logical interface, `ip.tun0:1`, is also configured. The logical interface has the source and destination IPv6 addresses specified by the `addif` command.

The contents of these configuration files are passed to `ifconfig` without change when the system is started in multiuser mode. The entries in [Example 10–11](#) are equivalent to the following:

```
# ifconfig ip.tun0 inet6 plumb
# ifconfig ip.tun0 inet6 tsrc 10.0.0.23 tdst 172.16.7.19 up
# ifconfig ip.tun0 inet6 addif 2001:db8:3b4c:1:5678:5678::2 up
```

The following shows the output of `ifconfig -a` for this tunnel.

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,
NONUD,IPv6> mtu 1480 index 6
    inet tunnel src 10.0.0.23  tunnel dst 172.16.7.19
    inet6 fe80::c0a8:6417/10 --> fe80::c0a8:713
ip.tun0:1: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NONUD,IPv6> mtu 1480
index 5
    inet6 2001:db8:3b4c:1:5678:5678::2
```

You can configure more logical interfaces by adding lines to the configuration file by using the following syntax:

```
addif IPv6-source IPv6-destination up
```

Note – When either end of the tunnel is an IPv6 router that advertises one or more prefixes over the tunnel, you do not need `addif` commands in the tunnel configuration files. Only `tsrc` and `tdst` might be required because all other addresses are autoconfigured.

In some situations, specific source and destination link-local addresses need to be manually configured for a particular tunnel. Change the first line of the configuration file to include these link-local addresses. The following line is an example:

```
tsrc 10.0.0.23 tdst 172.16.7.19 fe80::1/10 fe80::2 up
```

Notice that the source link-local address has a prefix length of 10. In this example, the `ip.tun0` interface resembles the following:

```
ip.tun0: flags=2200850<UP,POINTOPOINT,RUNNING,MULTICAST,NOUD,IPv6> mtu 1480
index 6
inet tunnel src 10.0.0.23 tunnel dst 172.16.7.19
inet6 fe80::1/10 --> fe80::2
```

To create a tunnel to encapsulate IPv6 packets over an IPv6 network, IPv6 over IPv6, you create the following file name:

```
/etc/hostname6.ip6.tun0
```

EXAMPLE 10-12 `hostname6.ip6.tun0` File for an IPv6 over IPv6 Tunnel

The following is an example of entries in the `hostname6.ip6.tun0` file for IPv6 encapsulation over an IPv6 network:

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
      tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
fe80::4 fe80::61 up
```

To create a tunnel to encapsulate IPv4 packets over an IPv6 network, IPv4 over IPv6, you would create the following file name:

```
/etc/hostname.ip6.tun0
```

EXAMPLE 10-13 `hostname.ip6.tun0` File for an IPv4 Over IPv6 Tunnel

The following is an example of entries in the `hostname.ip6.tun0` file for IPv4 encapsulation over an IPv6 network:

EXAMPLE 10-13 `hostname.ip6.tun0` File for an IPv4 Over IPv6 Tunnel (Continued)

```
tsrc 2001:db8:3b4c:114:a00:20ff:fe72:668c
      tdst 2001:db8:15fa:25:a00:20ff:fe9b:a1c3
10.0.0.4 10.0.0.61 up
```

To create a tunnel to encapsulate IPv4 packets over an IPv4 network, IPv4 over IPv4, you would create the following file name:

```
/etc/hostname.ip.tun0
```

EXAMPLE 10-14 `hostname.ip.tun0` for an IPv4 Over IPv4 Tunnel

The following is an example of entries in the `hostname.ip.tun0` file for IPv4 encapsulation over an IPv4 network:

```
tsrc 172.16.86.158 tdst 192.168.86.122
10.0.0.4 10.0.0.61 up
```

For specific information about `tun`, see the `tun(7M)` man page. For a general description of tunneling concepts during the transition to IPv6, see [“Overview of IPv6 Tunnels” on page 83](#). For a description of procedures for configuring tunnels, see [“Tasks for Configuring Tunnels for IPv6 Support \(Task Map\)” on page 129](#).

6to4 Automatic Tunnels

The Solaris OS includes 6to4 tunnels as a preferred interim method for making the transition from IPv4 to IPv6 addressing. 6to4 tunnels enable isolated IPv6 sites to communicate across an automatic tunnel over an IPv4 network that does not support IPv6. To use 6to4 tunnels, you must configure a boundary router on your IPv6 network as one endpoint of the 6to4 automatic tunnel. Thereafter, the 6to4 router can participate in a tunnel to another 6to4 site, or, if required, to a native IPv6, non-6to4 site.

This section provides reference materials on the following 6to4 topics:

- Topology of the 6to4 tunnel
- 6to4 addressing, including the format of the advertisement
- Description of packet flow across a 6to4 tunnel
- Topology of a tunnel between a 6to4 router and a 6to4 relay router
- Points to consider before you configure 6to4 relay router support

More information about 6to4 routing is available from the following sources.

Task or Detail	For Information
Tasks for configuring a 6to4 tunnel	“How to Configure a 6to4 Tunnel” on page 133
6to4-related RFC	RFC 3056, "Connection of IPv6 Domains via IPv4 Clouds" (ftp://ftp.rfc-editor.org/in-notes/rfc3056.txt)
Detailed information about the <code>6to4relay</code> command, which enables support for tunnels to a 6to4 relay router	<code>6to4relay(1M)</code> man page
6to4 security issues	Internet Draft, "Security Considerations for 6to4"

Topology of a 6to4 Tunnel

The following figure shows a 6to4 tunnel between two 6to4 sites.

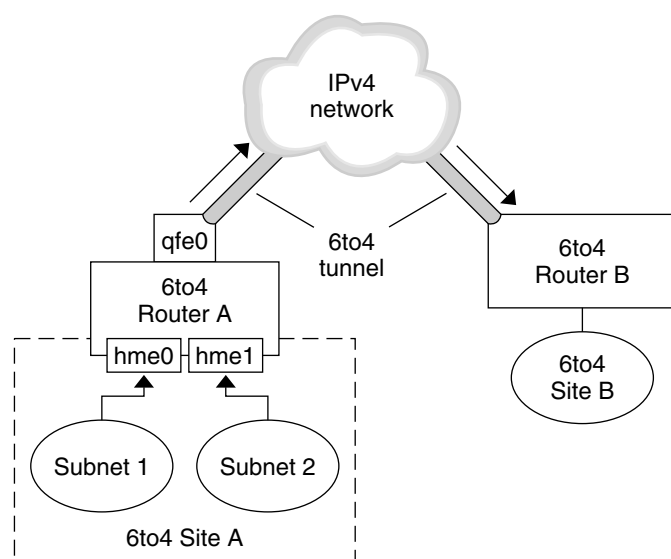


FIGURE 10-6 Tunnel Between Two 6to4 Sites

The figure depicts two isolated 6to4 networks, Site A and Site B. Each site has configured a router with an external connection to an IPv4 network. A 6to4 tunnel across the IPv4 network connects the 6to4 sites.

Before an IPv6 site can become a 6to4 site, you must configure at least one router interface for 6to4 support. This interface must provide the external connection to the IPv4 network. The address that you configure on `qfe0` must be globally unique. In this figure, boundary Router A's interface `qfe0` connects Site A to the IPv4 network. Interface `qfe0` must already be configured with an IPv4 address before you can configure `qfe0` as a 6to4 pseudo-interface.

In the figure, 6to4 Site A is composed of two subnets, which are connected to interfaces `hme0` and `hme1` on Router A. All IPv6 hosts on either subnet of Site A automatically reconfigure with 6to4-derived addresses on receipt of the advertisement from Router A.

Site B is the opposite endpoint of the tunnel from Site A. To correctly receive traffic from Site A, a boundary router on Site B must be configured for 6to4 support. Otherwise, packets that the router receives from Site A are not recognized and dropped.

Packet Flow Through the 6to4 Tunnel

This section describes the path of packets from a host at one 6to4 site to a host in a remote 6to4 site. This scenario uses the topology that is shown in [Figure 10-6](#). Moreover, the scenario assumes that the 6to4 routers and 6to4 hosts are already configured.

1. A host on Subnet 1 of 6to4 Site A sends a transmission, with a host at 6to4 Site B as the destination. Each packet header in the flow has a source 6to4-derived address and destination 6to4-derived address.
2. 6to4 Router A receives the outgoing packets and creates a tunnel over an IPv4 network to 6to4 Site B.
3. Site A's router encapsulates each 6to4 packet into an IPv4 header. Then the router uses standard IPv4 routing procedures to forward the packet over the IPv4 network.
4. Any IPv4 routers that the packets encounter use the packets' destination IPv4 address for forwarding. This address is the globally unique IPv4 address of the interface on Router B, which also serves as the 6to4 pseudo-interface.
5. Packets from Site A arrive at Router B, which decapsulates the IPv6 packets from the IPv4 header.
6. Router B then uses the destination address in the IPv6 packet to forward the packets to the recipient host at Site B.

Considerations for Tunnels to a 6to4 Relay Router

6to4 relay routers function as endpoints for tunnels from 6to4 routers that need to communicate with native IPv6, non-6to4 networks. Relay routers are essentially bridges between the 6to4 site and native IPv6 sites. Because this solution is very insecure, by default, the Solaris OS does not enable 6to4 relay router support. However, if your site requires such a tunnel, you use the `6to4relay` command to enable the following tunneling scenario.

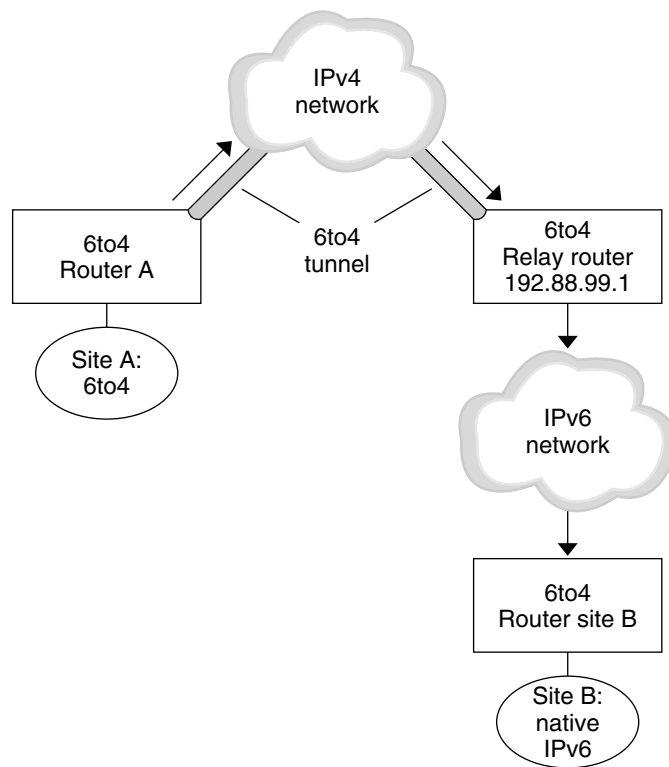


FIGURE 10-7 Tunnel From a 6to4 Site to a 6to4 Relay Router

In [Figure 10-7](#), 6to4 Site A needs to communicate with a node at the native IPv6 Site B. The figure shows the path of traffic from Site A onto a 6to4 tunnel over an IPv4 network. The tunnel has 6to4 Router A and a 6to4 relay router as its endpoints. Beyond the 6to4 relay router is the IPv6 network, to which IPv6 Site B is connected.

Packet Flow Between a 6to4 Site and Native IPv6 Site

This section describes the flow of packets from a 6to4 site to a native IPv6 site. The text uses the scenario that is shown in [Figure 10-7](#) as an example.

1. A host on 6to4 Site A sends a transmission that specifies as the destination a host at native IPv6 Site B. Each packet header in the flow has a 6to4-derived address as its source address. The destination address is a standard IPv6 address.
2. 6to4 Router A receives the outgoing packets and creates a tunnel over an IPv4 network to a 6to4 relay router.

6to4 relay routers that are part of the 6to4 relay router anycast group have the address 192 . 88 . 99 . 1. This anycast address is the default address for 6to4 relay routers. If you need to use a specific 6to4 relay router, you can override the default and specify that router's IPv4 address.

3. Site A's 6to4 router encapsulates each packet into a IPv4 header, which has the IPv4 address of the 6to4 relay router as its destination. The 6to4 router uses standard IPv4 routing procedures to forward the packet over the IPv4 network. Any IPv4 routers that the packets encounter forward the packets to the 6to4 relay router.
4. The physically closest anycast 6to4 relay router to Site A retrieves the packets that are destined for the 192.88.99.1 anycast group.
5. The relay router decapsulates the IPv4 header from the 6to4 packets, revealing the native IPv6 destination address.
6. The relay router then sends the now IPv6-only packets onto the IPv6 network, where the packets are ultimately retrieved by a router at Site B. The router then forwards the packets to the destination IPv6 node.

IPv6 Extensions to Solaris Name Services

This section describes naming changes that were introduced by the implementation of IPv6. You can store IPv6 addresses in any of the Solaris naming services, NIS, LDAP, DNS, and files. You can also use NIS over IPv6 RPC transports to retrieve any NIS data.

ipnodes Database

The `/etc/inet/ipnodes` file stores both IPv4 and IPv6 addresses. This file serves as a local database that associates the names of hosts with their IPv4 and IPv6 addresses. You should not store host names and their addresses in static files, such as `/etc/inet/ipnodes`. However, for testing purposes, store IPv6 addresses in a file in the same way that IPv4 addresses are stored in `/etc/inet/hosts`. The `ipnodes` file uses the same format convention as the `hosts` file. For more information on `/etc/inet/hosts`, refer to “[hosts Database](#)” on page 185. See the `ipnodes(4)` man page for a description of the `ipnodes` file.

IPv6-enabled applications use the `/etc/inet/ipnodes` database. The existing `/etc/hosts` database, which contains only IPv4 addresses, remains the same to facilitate existing applications. If the `ipnodes` database does not exist, IPv6-enabled applications use the existing `hosts` database.

Note – If you need to add addresses, you must add IPv4 addresses to both the `hosts` and `ipnodes` files. You add only IPv6 addresses to the `ipnodes` file.

EXAMPLE 10-15 `/etc/inet/ipnodes` File

You must group host name addresses by the host name, as shown in this example.

EXAMPLE 10-15 /etc/inet/ipnodes File (Continued)

```
#
# Internet IPv6 host table
# with both IPv4 and IPv6 addresses
#
::1      localhost
2001:db8:3b4c:114:a00:20ff:fe78:f37c  farsite.com farsite farsite-v6
fe80::a00:20ff:fe78:f37c      farsite-11.com farsitell
192.168.85.87                  farsite.com farsite farsite-v4
2001:db8:86c0:32:a00:20ff:fe87:9aba  nearsite.com nearsite nearsite-v6
fe80::a00:20ff:fe87:9aba      nearsite-11.com nearsitell
10.0.0.177                     nearsite.com nearsite nearsite-v4 loghost
```

DNS Extensions for IPv6

An IPv6-specific resource record, the AAAA resource record, has been specified by in RFC 1886 *DNS Extensions to Support IP Version 6*. This AAAA record maps a host name into a 128 bit IPv6 address. The PTR record is still used with IPv6 to map IP addresses into host names. The 32 four bit nibbles of the 128 bit address are reversed for an IPv6 address. Each nibble is converted to its corresponding hexadecimal ASCII value. Then, `ip6.int` is appended.

NIS Extensions for IPv6

Two new maps have been added for NIS: `ipnodes.byname` and `ipnodes.byaddr`. Similar to `/etc/inet/ipnodes`, these maps contain both IPv4 and IPv6 information. The `hosts.byname` and `hosts.byaddr` maps contain only IPv4 information. These maps remain the same to facilitate existing applications.

Changes to the `nsswitch.conf` File

In addition to the capability of looking up IPv6 addresses through `/etc/inet/ipnodes`, IPv6 support has been added to the NIS, LDAP, and DNS name services. Consequently, the `nsswitch.conf` file has been modified to support IPv6 lookups. An `ipnodes` line has been added to the `/etc/nsswitch.conf` file. This addition enables you to perform lookups in the new databases for each Solaris name service: NIS, LDAP, DNS, and files. The following bold line shows an example of the `ipnodes` entry:

```
hosts:  files dns nisplus [NOTFOUND=return]
ipnodes: files dns nisplus [NOTFOUND=return]
```

Note – Before changing the `/etc/nsswitch.conf` file to search `ipnodes` in multiple name services, populate these `ipnodes` databases with IPv4 and IPv6 addresses. Otherwise, unnecessary delays can result in the resolution of host addresses, including possible boot-timing delays.

The following diagram shows the new relationship between the `nsswitch.conf` file and the new name services databases for applications that use the `gethostbyname` and `getipnodebyname` commands. Items in italics are new. The `gethostbyname` command checks only for IPv4 addresses that are stored in `/etc/inet/hosts`. The `getipnodebyname` command consults the database that is specified in the `ipnodes` entry in the `nsswitch.conf` file. If the lookup fails, then the command checks the database that is specified in the `hosts` entry in the `nsswitch.conf` file.

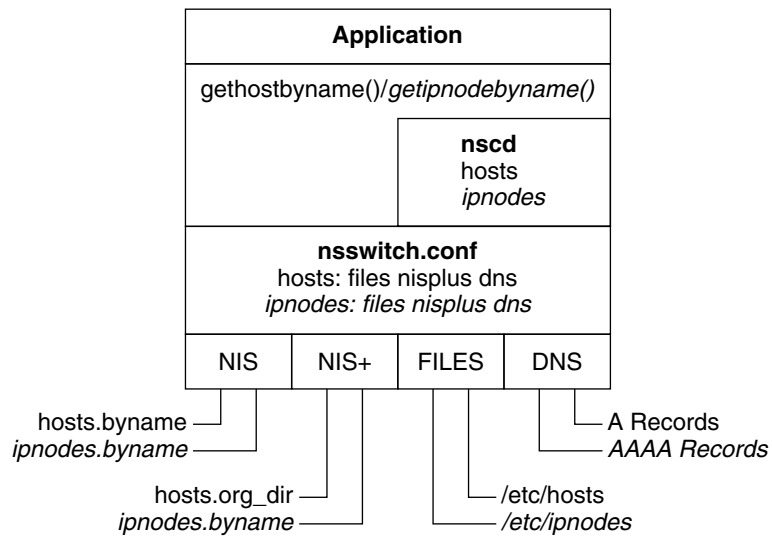


FIGURE 10-8 Relationship Between `nsswitch.conf` and Name Services

For more information on name services, see *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Changes to Name Service Commands

To support IPv6, you can look up IPv6 addresses with the existing name service commands. For example, the `ypmatch` command works with the new NIS maps. The `nslookup` command can look up the new AAAA records in DNS.

NFS and RPC IPv6 Support

NFS software and Remote Procedure Call (RPC) software support IPv6 in a seamless manner. Existing commands that are related to NFS services have not changed. Most RPC applications also run on IPv6 without any change. Some advanced RPC applications with transport knowledge might require updates.

IPv6 Over ATM Support

The Solaris OS supports IPv6 over ATM, permanent virtual circuits (PVC), and static switched virtual circuits (SVC).

PART III DHCP

This part contains conceptual information about the Dynamic Host Configuration Protocol (DHCP), and tasks for planning, configuring, administering, and troubleshooting the Solaris DHCP service.

About Solaris DHCP (Overview)

This chapter introduces the Dynamic Host Configuration Protocol (DHCP), and explains the concepts that underlie the protocol. This chapter also describes the advantages of using DHCP in your network.

This chapter contains the following information:

- “About the DHCP Protocol” on page 247
- “Advantages of Using Solaris DHCP” on page 248
- “How DHCP Works” on page 249
- “Solaris DHCP Server” on page 252
- “Solaris DHCP Client” on page 261

About the DHCP Protocol

The DHCP protocol enables host systems in a TCP/IP network to be configured automatically for the network as the systems boot. DHCP uses a client-server mechanism. Servers store and manage configuration information for clients and provide that information upon a client’s request. The information includes the client’s IP address and information about network services that are available to the client.

DHCP evolved from an earlier protocol, BOOTP, which was designed for booting over a TCP/IP network. DHCP uses the same format as BOOTP for messages between the client and server. However, unlike BOOTP messages, DHCP messages can include network configuration data for the client.

A primary benefit of DHCP is its ability to manage IP address assignments through leases. *Leases* allow IP addresses to be reclaimed when they are not in use. The reclaimed IP addresses can be reassigned to other clients. A site that uses DHCP can use a smaller pool of IP addresses than would be needed if all clients were assigned a permanent IP address.

Advantages of Using Solaris DHCP

DHCP relieves you of some of the time-consuming tasks involved in setting up a TCP/IP network and in the daily management of that network. Note that Solaris DHCP works only with IPv4.

Solaris DHCP offers the following advantages:

- **IP address management** – A primary advantage of DHCP is easier management of IP addresses. In a network without DHCP, you must manually assign IP addresses. You must be careful to assign unique IP addresses to each client and to configure each client individually. If a client moves to a different network, you must make manual modifications for that client. When DHCP is enabled, the DHCP server manages and assigns IP addresses without administrator intervention. Clients can move to other subnets without manual reconfiguration because they obtain, from a DHCP server, new client information appropriate for the new network.
- **Centralized network client configuration** – You can create a tailored configuration for certain clients, or for certain types of clients. The configuration information is stored in one place, in the DHCP data store. You do not need to log in to a client to change its configuration. You can make changes for multiple clients just by changing the information in the data store.
- **Support of BOOTP clients** – Both BOOTP servers and DHCP servers listen and respond to broadcasts from clients. The DHCP server can respond to requests from BOOTP clients as well as DHCP clients. BOOTP clients receive an IP address and the information needed to boot from a server.
- **Support of local clients and remote clients** – BOOTP provides for the relaying of messages from one network to another network. DHCP takes advantage of the BOOTP relay feature in several ways. Most network routers can be configured to act as BOOTP relay agents to pass BOOTP requests to servers that are not on the client's network. DHCP requests can be relayed in the same manner because, to the router, DHCP requests are indistinguishable from BOOTP requests. The Solaris DHCP server can also be configured to behave as a BOOTP relay agent, if a router that supports BOOTP relay is not available.
- **Network booting** – Clients can use DHCP to obtain the information that is needed to boot from a server on the network, instead of using RARP (Reverse Address Resolution Protocol) and the `bootparams` file. The DHCP server can give a client all the information that the client needs to function, including IP address, boot server, and network configuration information. Because DHCP requests can be relayed across subnets, you can deploy fewer boot servers in your network when you use DHCP network booting. RARP booting requires that each subnet have a boot server.
- **Large network support** – Networks with millions of DHCP clients can use Solaris DHCP. The DHCP server uses multithreading to process many client requests simultaneously. The server also supports data stores that are optimized to handle

large amounts of data. Data store access is handled by separate processing modules. This data store approach enables you to add support for any database that you require.

How DHCP Works

You must first install and configure the DHCP server. During configuration, you specify information about the network that clients need to operate on the network. After this information is in place, clients are able to request and receive network information.

The sequence of events for DHCP service is shown in the following diagram. The numbers in circles correlate to the numbered items in the description following the diagram.

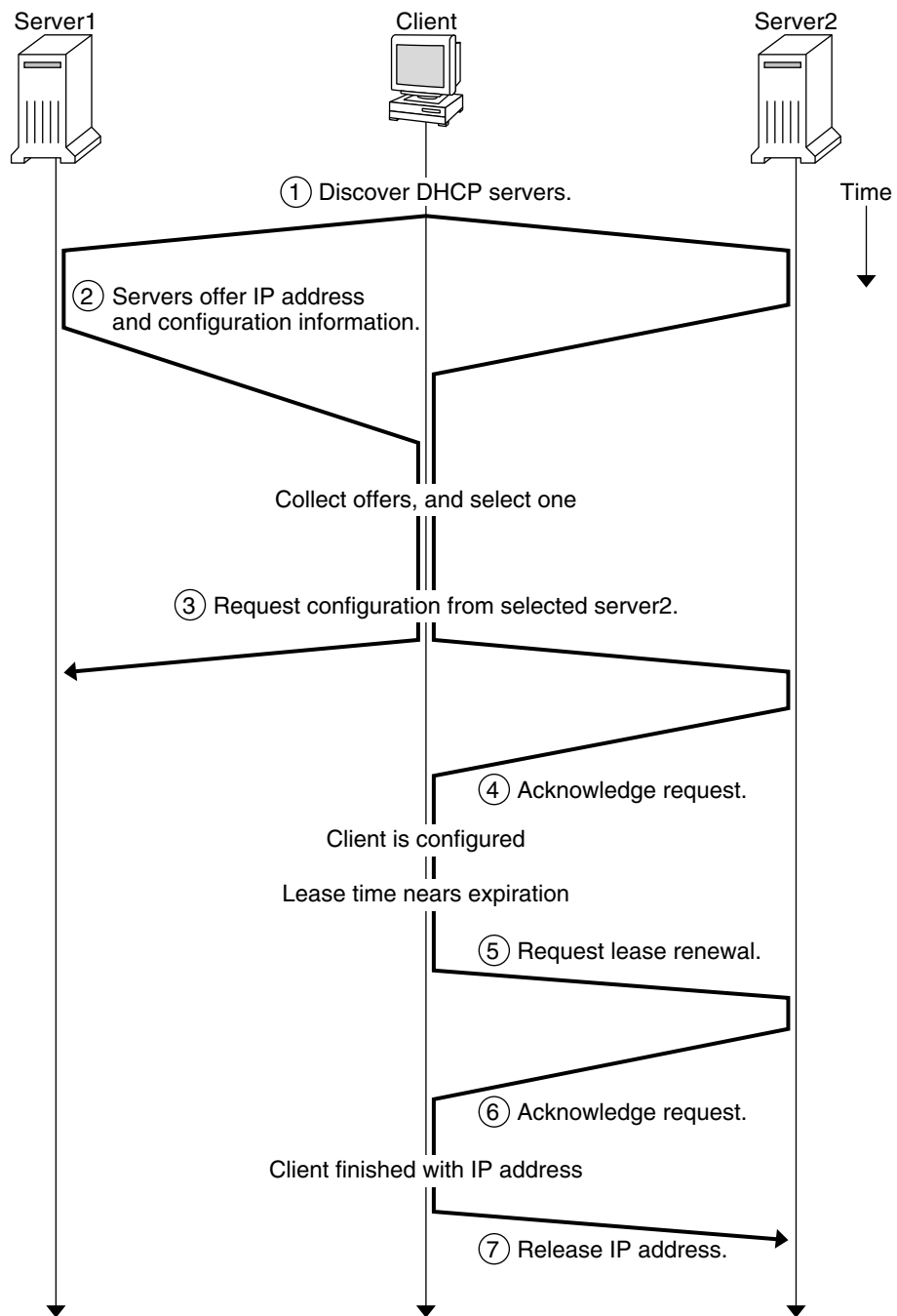


FIGURE 11-1 Sequence of Events for DHCP Service

The preceding diagram shows the following steps:

1. The client discovers a DHCP server by broadcasting a *discover message* to the limited broadcast address (255 . 255 . 255 . 255) on the local subnet. If a router is present and configured to behave as a BOOTP relay agent, the request is passed to other DHCP servers on different subnets. The client's *broadcast* includes its unique ID, which, in the Solaris DHCP implementation, is derived from the client's Media Access Control (MAC) address. On an Ethernet network, the MAC address is the same as the Ethernet address.

DHCP servers that receive the discover message can determine the client's network by looking at the following information:

- Which network interface did the request come in on? The server determines either that the client is on the network to which the interface is connected, or that the client is using a BOOTP relay agent connected to that network.
 - Does the request include the IP address of a BOOTP relay agent? When a request passes through a relay agent, the relay agent inserts its address in the request header. When the server detects a *relay agent address*, the server knows that the network portion of the address indicates the client's network address because the relay agent must be connected to the client's network.
 - Is the client's network subnetted? The server consults the `netmasks` table to find the subnet mask used on the network indicated by the relay agent's address or by the address of the network interface that received the request. Once the server knows the subnet mask used, it can determine which portion of the network address is the host portion, and then it can select an IP address appropriate for the client. See the `netmasks(4)` man page for information on `netmasks`.
2. After the DHCP servers determine the client's network, the servers select an appropriate IP address and verify that the address is not already in use. The DHCP servers then respond to the client by broadcasting an *offer message*. The offer message includes the selected IP address and information about services that can be configured for the client. Each server temporarily reserves the offered IP address until the client determines whether to use the IP address.
 3. The client selects the best offer, based on the number and type of services offered. The client broadcasts a request that specifies the IP address of the server that made the best offer. The broadcast ensures that all the responding DHCP servers know that the client has chosen a server. The servers that are not chosen can cancel the reservations for the IP addresses that they had offered.
 4. The selected server allocates the IP address for the client and stores the information in the DHCP data store. The server also sends an acknowledgement message (ACK) to the client. The *acknowledgement message* contains the network configuration parameters for the client. The client uses the `ping` utility to test the IP address to make sure no other system is using it. The client then continues booting to join the network.
 5. The client monitors the lease time. When a set period of time has elapsed, the client sends a new message to the chosen server to increase the lease time.

6. The DHCP server that receives the request extends the lease time if the lease still adheres to the local lease policy set by the administrator. If the server does not respond within 20 seconds, the client broadcasts a request so that one of the other DHCP servers can extend the lease.
7. When the client no longer needs the IP address, the client notifies the server that the IP address is released. This notification can happen during an orderly shutdown and can also be done manually.

Solaris DHCP Server

The Solaris DHCP server runs as a daemon in the Solaris Operating System (Solaris OS) on a host system. The server has two basic functions:

- **Managing IP addresses** – The DHCP server controls a range of IP addresses and allocates them to clients, either permanently or for a defined period of time. The server uses a lease mechanism to determine how long a client can use a nonpermanent address. When the address is no longer in use, it is returned to the pool and can be reassigned. The server maintains information about the binding of IP addresses to clients in its DHCP network tables, ensuring that no address is used by more than one client.
- **Providing network configuration for clients** – The server assigns an IP address and provides other information for network configuration, such as a host name, broadcast address, network subnet mask, default gateway, name service, and potentially much more information. The network configuration information is obtained from the server's `dhcptab` database.

The Solaris DHCP server can also be configured to perform the following additional functions:

- **Responding to BOOTP client requests** – The server listens for broadcasts from BOOTP clients discovering a BOOTP server and provides them with an IP address and boot parameters. The information must have been configured statically by an administrator. The DHCP server can simultaneously perform as a BOOTP server and as a DHCP server.
- **Relaying requests** – The server relays BOOTP and DHCP requests to appropriate servers on other subnets. The server cannot provide DHCP or BOOTP service when configured as a BOOTP relay agent.
- **Providing network booting support for DHCP clients** – The server can provide DHCP clients with information needed to boot over the network: an IP address, boot parameters, and network configuration information. The server can also provide information that DHCP clients need to boot and install over a wide area network (WAN).
- **Updating DNS tables for clients that supply a host name** – For clients that provide a `Hostname` option and value in their requests for DHCP service, the server can attempt DNS updates on their behalf.

DHCP Server Management

As superuser, you can start, stop, and configure the DHCP server with DHCP Manager or with command-line utilities described in “[DHCP Command-Line Utilities](#)” on page 255. Generally, the DHCP server is configured to start automatically when the system boots, and to stop when the system is shut down. You should not need to start and stop the server manually under normal conditions.

DHCP Data Store

All the data used by the Solaris DHCP server is maintained in a data store. The data store might consist of plain text files, NIS+ tables, or binary-format files. While configuring the DHCP service, you choose the type of data store to be used. The section “[Choosing the DHCP Data Store](#)” on page 269 describes the differences between the types of data stores. You can convert a data store from one format to another by using DHCP Manager or the `dhcpcnfig` command.

You can also move data from one DHCP server’s data store to another server’s data store. You can use export and import utilities that work with the data stores, even if the servers are using different data store formats. You can export and import the entire content of a data store, or just some of the data within it, using DHCP Manager or the `dhcpcnfig` command.

Note – Any database or file format can be used for DHCP data storage if you develop your own code module to provide an interface between Solaris DHCP (server and management tools) and the database. For more information, see the *Solaris DHCP Service Developer’s Guide*.

Within the Solaris DHCP data store are two types of tables. You can view and manage the contents of these tables by using either DHCP Manager or the command-line utilities. The data tables are as follows:

- **dhcptab table** – Table of configuration information that can be passed to clients.
- **DHCP network tables** – Tables containing information about the DHCP and BOOTP clients that reside on the network specified in the table name. For example, the network 192.168.32.0 would have a table whose name includes 192_168_32_0.

The dhcptab Table

The `dhcptab` table contains all the information that clients can obtain from the DHCP server. The DHCP server scans the `dhcptab` table each time it starts. The file name of the `dhcptab` table varies according to the data store used. For example, the `dhcptab` table created by the NIS+ data store `SUNWnisplus` is `SUNWnisplus1_dhcptab`.

The DHCP protocol defines a number of standard items of information that can be passed to clients. These items are referred to as parameters, symbols, or options. Options are defined in the DHCP protocol by numeric codes and text labels, but without values. Some commonly used standard options are shown in the following table.

TABLE 11-1 Sample DHCP Standard Options

Code	Label	Description
1	Subnet	Subnet mask IP address
3	Router	IP address for the router
6	DNSserv	IP address for the DNS server
12	Hostname	Text string for the client host name
15	DNSdomain	DNS domain name

Some options are automatically assigned values when you provide information during server configuration. You can also explicitly assign values to other options at a later time. Options and their values are passed to the client to provide configuration information. For example, the option/value pair, `DNSdomain=Georgia.Peach.COM`, sets the client's DNS domain name to `Georgia.Peach.COM`.

Options can be grouped with other options in containers known as *macros*, which makes it easier to pass information to a client. Some macros are created automatically during server configuration and contain options that were assigned values during configuration. Macros can also contain other macros.

The format of the `dhcptab` table is described in the `dhcptab(4)` man page. In DHCP Manager, all the information shown in the Options and Macros tabs comes from the `dhcptab` table. See "About DHCP Options" on page 258 for more information about options. See "About DHCP Macros" on page 259 for more information about macros.

Note that the `dhcptab` table should not be edited manually. You should use either the `dhtadm` command or DHCP Manager to create, delete, or modify options and macros.

DHCP Network Tables

A DHCP network table maps client identifiers to IP addresses and the configuration parameters associated with each address. The format of the network tables is described in the `dhcp_network(4)` man page. In DHCP Manager, all the information shown in the Addresses tab comes from the network tables.

DHCP Manager

DHCP Manager is a graphical user interface (GUI) tool you can use to perform all management duties associated with the DHCP service. You can use it to manage the server as well as the data the server uses. You must be superuser when you run DHCP Manager.

You can use DHCP Manager with the server in the following ways:

- Configuring and unconfiguring the DHCP server
- Starting, stopping, and restarting the DHCP server
- Disabling and enabling DHCP service
- Customizing DHCP server settings

DHCP Manager enables you to manage the IP addresses, network configuration macros, and network configuration options in the following ways:

- Adding and deleting networks under DHCP management
- Viewing, adding, modifying, deleting, and releasing IP addresses under DHCP management
- Viewing, adding, modifying, and deleting network configuration macros
- Viewing, adding, modifying, and deleting nonstandard network configuration options

DHCP Manager allows you to manage the DHCP data stores in the following ways:

- Convert data to a new data store format
- Move DHCP data from one DHCP server to another by exporting it from the first server and importing it on the second server

DHCP Manager includes extensive online help for procedures you can perform with the tool. For more information, see [“About DHCP Manager” on page 292](#).

DHCP Command-Line Utilities

All DHCP management functions can be performed by using command-line utilities. You can run the utilities if you are logged in as superuser or as a user assigned to the DHCP Management profile. See [“Setting Up User Access to DHCP Commands” on page 295](#).

The following table lists the utilities and describes the purpose of each utility.

TABLE 11–2 DHCP Command-Line Utilities

Command	Description and Purpose	Man Page Links
<code>in.dhcpd</code>	The DHCP service daemon. Command-line arguments enable you to set several runtime options.	<code>in.dhcpd(1M)</code>
<code>dhcpconfig</code>	Used to configure and unconfigure a DHCP server. This utility enables you to perform many of the functions of DHCP Manager from the command line. This utility is primarily intended for use in scripts for sites that want to automate some configuration functions. <code>dhcpconfig</code> collects information from the server system’s network topology files to create useful information for the initial configuration.	<code>dhcpconfig(1M)</code>
<code>dhtadm</code>	Used to add, delete, and modify configuration options and macros for DHCP clients. This utility lets you edit the <code>dhcptab</code> table indirectly, which ensures the correct format of the <code>dhcptab</code> table. You should not directly edit the <code>dhcptab</code> table.	<code>dhtadm(1M)</code>
<code>pntadm</code>	Used to manage the DHCP network tables. You can use this utility to perform the following tasks: <ul style="list-style-type: none"> ■ Add and remove IP addresses and networks under DHCP management. ■ Modify the network configuration for specified IP addresses. ■ Display information about IP addresses and networks under DHCP management. 	<code>pntadm(1M)</code>

Role-Based Access Control for DHCP Commands

Security for the `dhcpconfig`, `dhtadm`, and `pntadm` commands is determined by role-based access control (RBAC) settings. By default, the commands can be run only by superuser. If you want to use the commands under another user name, you must assign the user name to the DHCP Management profile as described in [“Setting Up User Access to DHCP Commands”](#) on page 295.

DHCP Server Configuration

You configure the Solaris DHCP server the first time you run DHCP Manager on the system where you want to run the DHCP server.

DHCP Manager server configuration dialog boxes prompt you for essential information needed to enable and run the DHCP server on one network. Some default values are obtained from existing system files. If you have not configured the system for the network, there are no default values. DHCP Manager prompts for the following information:

- Role of the server, either as the DHCP server or as the BOOTP relay agent
- Data store type (files, binary files, NIS+, or something specific to your site)
- Data store configuration parameters for the data store type you selected
- Name service to use to update host records, if any (`/etc/hosts`, NIS+, or DNS)
- Length of lease time and whether clients should be able to renew leases
- DNS domain name and IP addresses of DNS servers
- Network address and subnet mask for the first network you want to configure for DHCP service
- Network type, either local area network (LAN) or point-to-point network
- Router discovery or the IP address of a particular router
- NIS domain name and IP address of NIS servers
- NIS+ domain name and IP address of NIS+ servers

You can also configure the DHCP server using the `dhcpconfig` command. This utility automatically gathers information from existing system files to provide a useful initial configuration. Therefore, you must ensure that the files are correct before running `dhcpconfig`. See the `dhcpconfig(1M)` man page for information about the files that `dhcpconfig` uses to obtain information.

IP Address Allocation

The Solaris DHCP server supports the following types of IP address allocation:

- **Manual allocation** – The server provides a specific IP address that you choose for a specific DHCP client. The address cannot be reclaimed or assigned to another client.
- **Automatic, or permanent, allocation** – The server provides an IP address that has no expiration time, making it permanently associated with the client until you change the assignment or the client releases the address.
- **Dynamic allocation** – The server provides an IP address to a requesting client, with a lease for a specific period of time. When the lease expires, the address is taken back by the server and can be assigned to another client. The period of time is determined by the lease time configured for the server.

Network Configuration Information

You determine what information to provide to DHCP clients. When you configure the DHCP server, you provide essential information about the network. Later, you can add more information that you want to provide to clients.

The DHCP server stores network configuration information in the `dhcptab` table, in the form of option/value pairs and macros. Options are keywords for network data that you want to supply to clients. Values are assigned to options and passed to clients in DHCP messages. For example, the NIS server address is passed by way of an option called `NISservs`. The `NISservs` option has a value that is equal to a list of IP addresses, which is assigned by the DHCP server. Macros provide a convenient way to group together any number of options that you want to supply to clients. You can use DHCP Manager to create macros to group options and to assign values to the options. If you prefer a command-line tool, you can use `dhtadm`, the DHCP configuration table management utility, to work with options and macros.

About DHCP Options

In Solaris DHCP, an *option* is a piece of network information to be passed to a client. The DHCP literature also refers to options as *symbols* or *tags*. An option is defined by a numeric code and a text label. An option receives a value when it is used in the DHCP service.

The DHCP protocol defines a large number of standard options for commonly specified network data: `Subnet`, `Router`, `Broadcst`, `NIS+dom`, `Hostname`, and `LeaseTim` are a few examples. A complete list of standard options is shown in the `dhcp_inittab(4)` man page. You cannot modify the standard option keywords in any way. However, you can assign values to the options that are relevant to your network when you include the options in macros.

You can create new options for data that is not represented by the standard options. Options you create must be classified in one of three categories:

- **Extended** – Reserved for options that have become standard DHCP options but are not yet included in the DHCP server implementation. You might use an extended option if you know of a standard option that you want to use, but you do not want to upgrade your DHCP server.
- **Site** – Reserved for options that are unique to your site. You create these options.
- **Vendor** – Reserved for options that should apply only to clients of a particular class, such as a hardware or vendor platform. The Solaris DHCP implementation includes a number of vendor options for Solaris clients. For example, the option `SrootIP4` is used to specify the IP address of a server that a client that boots from the network should use for its root (`/`) file system.

[Chapter 14](#) includes procedures for creating, modifying, and deleting DHCP options.

About DHCP Macros

In the Solaris DHCP service, a *macro* is a collection of network configuration options and the values that you assign to them. Macros are created to group options together to be passed to specific clients or types of clients. For example, a macro intended for all clients of a particular subnet might contain option/value pairs for subnet mask, router IP address, broadcast address, NIS+ domain, and lease time.

Macro Processing by the DHCP Server

When the DHCP server processes a macro, it places the network options and values defined in the macro in a DHCP message to a client. The server processes some macros automatically for clients of a particular type.

For the server to process a macro automatically, the name of the macro must comply with one of the categories shown in the following table.

TABLE 11-3 DHCP Macro Categories for Automatic Processing

Macro Category	Description
Client class	The macro name matches a class of client, indicated by the client machine type, operating system, or both. For example, if a server has a macro named <code>SUNW.Sun-Blade-100</code> , any client whose hardware implementation is <code>SUNW.Sun-Blade-100</code> automatically receives the values in the <code>SUNW.Sun-Blade-100</code> macro.
Network address	The macro name matches a DHCP-managed network IP address. For example, if a server has a macro named <code>10.53.224.0</code> , any client connected to the <code>10.53.224.0</code> network automatically receives the values in the <code>10.53.224.0</code> macro.
Client ID	The macro name matches some unique identifier for the client, usually derived from an Ethernet or MAC address. For example, if a server has a macro named <code>08002011DF32</code> , the client with the client ID <code>08002011DF32</code> (derived from the Ethernet address <code>8:0:20:11:DF:32</code>) automatically receives the values in the macro named <code>08002011DF32</code> .

A macro with a name that does not use one of the categories listed in [Table 11-3](#) can be processed only if one of the following is true:

- The macro is mapped to an IP address.
- The macro is included in another macro that is processed automatically.
- The macro is included in another macro that is mapped to an IP address.

Note – When you configure a server, a macro that is named to match the server’s name is created by default. This server macro is *not* processed automatically for any client because it is not named with one of the name types that cause automatic processing. When you later create IP addresses on the server, the IP addresses are mapped to use the server macro by default.

Order of Macro Processing

When a DHCP client requests DHCP services, the DHCP server determines which macros match the client. The server processes the macros, using the macro categories to determine the order of processing. The most general category is processed first, and the most specific category is processed last. The macros are processed in the following order:

1. Client class macros – The most general category
2. Network address macros – More specific than Client class
3. Macros mapped to IP addresses – More specific than Network address
4. Client ID macros – The most specific category, pertaining to one client

A macro that is included in another macro is processed as part of the container macro.

If the same option is included in more than one macro, the value for that option in the macro with the most specific category is used because it is processed last. For example, if a Network address macro contains the lease time option with a value of 24 hours, and a Client ID macro contains the lease time option with a value of 8 hours, the client receives a lease time of 8 hours.

Size Limit for DHCP Macros

The sum total of the values assigned to all the options in a macro must not exceed 255 bytes, including the option codes and length information. This limit is dictated by the DHCP protocol.

The macros that are most likely to be impacted by this limit are macros that are used to pass paths to files on Solaris installation servers. Generally, you should pass the minimum amount of vendor information needed. You should use short path names in options that require path names. If you create symbolic links to long paths, you can pass the shorter link names.

Solaris DHCP Client

The term “client” is sometimes used to refer to a physical machine that is performing a client role on the network. However, the DHCP client described in this document is a software entity. The Solaris DHCP client is a daemon (`dhcpgent`) that runs in the Solaris OS on a system that is configured to receive its network configuration from a DHCP server. DHCP clients from other vendors can also use the services of the Solaris DHCP server. However, this document describes only the Solaris DHCP client.

See [Chapter 15](#) for detailed information about the Solaris DHCP client.

Planning for DHCP Service (Tasks)

You can use the DHCP service in a network that you are creating or in a network that exists. If you are setting up a network, see [Chapter 2](#) before you attempt to set up the DHCP service. If the network already exists, continue in this chapter.

This chapter describes what you need to do before you set up the DHCP service on your network. The information is intended for use with DHCP Manager, although you can also use the command-line utility `dhcpconfig` to set up the DHCP service.

This chapter contains the following information:

- “Preparing Your Network for the DHCP Service (Task Map)” on page 263
- “Making Decisions for Your DHCP Server Configuration (Task Map)” on page 268
- “Making Decisions for IP Address Management (Task Map)” on page 271
- “Planning for Multiple DHCP Servers” on page 274
- “Planning DHCP Configuration of Your Remote Networks” on page 275
- “Selecting the Tool for Configuring DHCP” on page 276

Preparing Your Network for the DHCP Service (Task Map)

Before you set up your network to use DHCP, you must collect information to help you make decisions for configuring one or more servers. Use the following task map to identify the tasks for preparing your network for DHCP.

Task	Description	For Instructions
Map your network topology.	Determine and locate the services that are available on the network.	“Mapping Your Network Topology” on page 264
Determine the number of DHCP servers you need.	Use the expected number of DHCP clients as a basis for determining the number of DHCP servers you need.	“Determining the Number of DHCP Servers” on page 265
Update system files and <code>netmasks</code> table.	Reflect the network topology accurately.	“Updating System Files and Netmask Tables” on page 266

Mapping Your Network Topology

If you have not already done so, you should map the physical structure of your network. Indicate the location of routers and clients, and the location of servers that provide network services. This map of your network topology can help you determine which server to use for the DHCP service. The map can also help you determine the configuration information that the DHCP server can provide to clients.

See [Chapter 2](#) for more information about planning your network.

The DHCP configuration process can gather some network information from the server’s system and network files. [“Updating System Files and Netmask Tables” on page 266](#) discusses these files. However, you might want to give clients other service information, which you must enter into the server’s macros. As you examine your network topology, record the IP addresses of any servers you want your clients to know about. The following servers, for example, might provide services on your network. The DHCP configuration does not discover these servers.

- Time server
- Log server
- Print server
- Install server
- Boot server
- Web proxy server
- Swap server
- X Window font server
- Trivial File Transfer Protocol (TFTP) server

Network Topology to Avoid

In some IP network environments, several local area networks (LANs) share the same network hardware media. The networks may use multiple network hardware interfaces or multiple logical interfaces. DHCP does not work well in this kind of

shared media network. When multiple LANs run across the same physical network, a DHCP client's request arrives on all network hardware interfaces. This effect makes the client appear to be attached to all of the IP networks simultaneously.

DHCP must be able to determine the address of a client's network in order to assign an appropriate IP address to the client. If more than one network is present on the hardware media, the server cannot determine the client's network. The server cannot assign an IP address without knowing the network number.

You can use DHCP on only one of the networks. If one network does not suit your DHCP needs, you must reconfigure the networks. You should consider the following suggestions:

- Use a variable length subnet mask (VLSM) on your subnets to make better use of the IP address space you have. You may not need to run multiple networks on the same physical network. See the `netmasks(4)` man page for information about implementing variable length subnetting. For more detailed information about Classless Inter-Domain Routing (CIDR) and VLSM, see <http://www.ietf.org/rfc/rfc1519.txt>.
- Configure the ports on your switches to assign devices to different physical LANs. This technique preserves the mapping of one LAN to one IP network, required for Solaris DHCP. See the documentation for the switch for information about port configuration.

Determining the Number of DHCP Servers

The data store option that you choose has a direct effect on the number of servers you must have to support your DHCP clients. The following table shows the maximum number of DHCP and BOOTP clients that can be supported by one DHCP server for each data store.

TABLE 12-1 Estimated Maximum Number of Clients Supported by One DHCP Server

Data Store Type	Maximum Number of Clients Supported
Text files	10,000
NIS+	40,000
Binary files	100,000

This maximum number is a general guideline, not an absolute number. A DHCP server's client capacity depends greatly on the number of transactions per second that the server must process. Lease times and usage patterns have a significant impact on the transaction rate. For example, suppose leases are set to 12 hours and users turn their systems off at night. If many users turn on their systems at the same time in the

morning, the server must handle transaction peaks as many clients request leases simultaneously. The DHCP server can support fewer clients in such an environment. The DHCP server can support more clients in an environment with longer leases, or an environment that consists of constantly connected devices such as cable modems.

The section “Choosing the DHCP Data Store” on page 269 compares the types of data stores.

Updating System Files and Netmask Tables

During DHCP configuration, the DHCP tools scan various system files on your server for information that can be used to configure the server.

You must be sure the information in the system files is current before you run DHCP Manager or `dhcpcfg` to configure your server. If you notice errors after you configure the server, use DHCP Manager or `dhtadm` to modify the macros on the server.

The following table lists some of the information gathered during DHCP server configuration, and the sources for the information. Be sure this information is set correctly on the server before you configure DHCP on the server. If you make changes to the system files after you configure the server, you should reconfigure the service to reflect these changes.

TABLE 12-2 Information Used for DHCP Configuration

Information	Source	Comments
Time zone	System date, time zone settings	The date and time zone are initially set during Solaris installation. You can change the date by using the <code>date</code> command. You can change the time zone by editing the <code>/etc/default/init</code> file to set the <code>TZ</code> environment variable. See the <code>TIMEZONE(4)</code> man page for more information.
DNS parameters	<code>/etc/resolv.conf</code>	The DHCP server uses the <code>/etc/resolv.conf</code> file to obtain DNS parameters such as the DNS domain name and DNS server addresses. See <i>System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)</i> or the <code>resolv.conf(4)</code> man page for more information about <code>resolv.conf</code> .

TABLE 12-2 Information Used for DHCP Configuration *(Continued)*

Information	Source	Comments
NIS or NIS+ parameters	System domain name, <code>nsswitch.conf</code> , NIS or NIS+	The DHCP server uses the <code>domainname</code> command to obtain the domain name of the server system. The <code>nsswitch.conf</code> file tells the server where to look for domain-based information. If the server system is an NIS or NIS+ client, the DHCP server performs a query to get NIS or NIS+ server IP addresses. See the <code>nsswitch.conf(4)</code> man page for more information.
Default router	System routing tables, user prompt	The DHCP server searches the network routing tables to find the default router for clients that are attached to the local network. For clients not on the same network, the DHCP server must prompt you for the information.
Subnet mask	Network interface, <code>netmasks</code> table	The DHCP server looks to its own network interfaces to determine the netmask and broadcast address for local clients. If the request was forwarded by a relay agent, the server obtains the subnet mask in the <code>netmasks</code> table on the relay agent's network.
Broadcast address	Network interface, <code>netmasks</code> table	For the local network, the DHCP server obtains the broadcast address by querying the network interface. For remote networks, the server uses the BOOTP relay agent's IP address and the remote network's netmask to calculate the broadcast address for the network.

Making Decisions for Your DHCP Server Configuration (Task Map)

This section discusses some of the decisions to make before you configure the first DHCP server on your network. Use this task map to identify the decisions that you must make.

Task	Description	For Instructions
Select a server for DHCP.	Determine if a server meets the system requirements to run the DHCP service.	“Selecting a Host to Run the DHCP Service” on page 268
Choose a data store.	Compare the data store types to determine the best data store for your site.	“Choosing the DHCP Data Store” on page 269
Set a lease policy.	Learn about IP address leases to help you determine appropriate lease policy for your site.	“Setting a Lease Policy” on page 269
Select a router address or router discovery.	Determine whether DHCP clients use router discovery or a specific router.	“Determining Routers for DHCP Clients” on page 270

Selecting a Host to Run the DHCP Service

With your network topology in mind, you can use the following system requirements to select a host on which to set up a DHCP server.

The host must meet the following requirements:

- The host must run the Solaris 2.6 release or later. If you need to support a large number of clients, you must install the Solaris 8 7/01 release or a later version.
- The host must be accessible to all the networks that have clients that plan to use DHCP, either directly on the network or through a BOOTP relay agent.
- The host must be configured to use routing.
- The host must have a correctly configured `netmasks` table that reflects your network topology.

Choosing the DHCP Data Store

You can choose to store the DHCP data in text files, binary files, or the NIS+ directory service. The following table summarizes the features of each type of data store, and indicates the environment in which to use each data store type.

TABLE 12-3 Comparison of DHCP Data Stores

Data Store Type	Performance	Maintenance	Sharing	Environment
Binary files	High performance, high capacity	Low maintenance, no database servers required. Contents must be viewed with DHCP Manager or <code>dhtadm</code> and <code>pntadm</code> . Regular file backups suggested.	Data stores cannot be shared among DHCP servers.	Midsized to large environments with many networks with thousands of clients per network. Useful for small to medium ISPs.
NIS+	Moderate performance and capacity, dependent upon NIS+ service's performance and capacity	DHCP server system must be configured as an NIS+ client. Requires NIS+ service maintenance. Contents must be viewed with DHCP Manager or <code>dhtadm</code> and <code>pntadm</code> . Regular backup with <code>nisbackup</code> is suggested.	DHCP data is distributed in NIS+, and multiple servers can access the same containers.	Small to midsized environments with up to 5000 clients per network.
Text files	Moderate performance, low capacity	Low maintenance, no database servers required. ASCII format is readable without DHCP Manager, <code>dhtadm</code> , or <code>pntadm</code> . Regular file backups suggested.	Data store can be shared among DHCP servers if DHCP data is stored on one file system that is exported through an NFS mount point.	Small environments with less than 10,000 clients, with a few hundred to a thousand clients per network.

Traditional NIS is not offered as a data store option because NIS does not support fast incremental updates. If your network uses NIS, you should use text files or binary files for your data store.

Setting a Lease Policy

A *lease* specifies the amount of time the DHCP server permits a DHCP client to use a particular IP address. During the initial server configuration, you must specify a site-wide lease policy. The *lease policy* indicates the lease time and specifies whether

clients can renew their leases. The server uses the information that you supply to set option values in the default macros that the server creates during configuration. You can set different lease policies for specific clients or type of clients, by setting options in configuration macros you create.

The *lease time* is specified as a number of hours, days, or weeks for which the lease is valid. When a client is assigned an IP address, or renegotiates a lease on an IP address, the lease expiration date and time is calculated. The number of hours in the lease time is added to the timestamp on the client's DHCP acknowledgement. For example, suppose the timestamp of the DHCP acknowledgment is September 16, 2005 9:15 A.M., and the lease time is 24 hours. The lease expiration time in this example is September 17, 2005 9:15 A.M. The lease expiration time is stored in the client's DHCP network record, viewable in DHCP Manager or with the `pntadmutility`.

The lease time value should be relatively small so that expired addresses are reclaimed quickly. The lease time value also should be large enough to outlast DHCP service disruptions. Clients should be able to function while the system that runs the DHCP service is repaired. A general guideline is to specify a time that is two times the predicted downtime of a system. For example, if you need four hours to obtain and replace a defective part and reboot the system, specify a lease time of eight hours.

The lease negotiation option determines whether a client can renegotiate its lease with the server before the lease expires. If lease negotiation is allowed, the client tracks the time that remains in its lease. When half of the lease time has passed, the client requests the DHCP server to extend its lease to the original lease time. You should disable lease negotiation in environments where there are more systems than IP addresses. The time limit is then enforced on the use of IP addresses. If there are enough IP addresses, you should enable lease negotiation to avoid forcing clients to take down their network interfaces when leases expire. If you make clients obtain new leases, the clients' TCP connections such as NFS and telnet sessions might be interrupted. You can enable lease negotiation for all clients during the server configuration. You can enable lease negotiation for particular clients or particular types of clients through the use of the `LeaseNeg` option in configuration macros.

Note – Systems that provide services on the network should retain their IP addresses. Such systems should not be subject to short-term leases. You can use DHCP with such systems if you assign reserved manual IP addresses to those systems, rather than IP addresses with permanent leases. You can then detect when the system's IP address is no longer in use.

Determining Routers for DHCP Clients

Host systems use routers for any network communication beyond their local network. The hosts must know the IP addresses of these routers.

When you configure a DHCP server, you must provide DHCP clients with router addresses in one of two ways. One way is to provide specific IP addresses for routers. However, the preferred method is to specify that clients should find routers with the router discovery protocol.

If clients on your network can perform router discovery, you should use the router discovery protocol, even if there is only one router. Router discovery enables a client to adapt easily to router changes in the network. For example, suppose that a router fails and is replaced by a router with a new address. Clients can discover the new address automatically without having to obtain a new network configuration to get the new router address.

Making Decisions for IP Address Management (Task Map)

As part of the DHCP service setup, you determine several aspects of the IP addresses that the server is to manage. If your network needs more than one DHCP server, you can assign responsibility for some IP addresses to each server. You must decide how to divide responsibility for the addresses. The following task map can help you make IP address management decisions.

Task	Description	For Information
Specify which addresses that the server should manage.	Determine how many addresses you want the DHCP server to manage, and what those addresses are.	“Number and Ranges of IP Addresses” on page 272
Decide if the server should automatically generate host names for clients.	Learn how client host names are generated so that you can decide whether to generate host names.	“Client Host Name Generation” on page 272
Determine what configuration macro to assign to clients.	Learn about client configuration macros so that you can select an appropriate macro for clients.	“Default Client Configuration Macros” on page 272
Determine lease types to use.	Learn about lease types to help you determine what type is best for your DHCP clients.	“Dynamic and Permanent Lease Types” on page 273

Number and Ranges of IP Addresses

During the initial server configuration, DHCP Manager allows you to add one block, or range, of IP addresses under DHCP management by specifying the total number of addresses and the first address in the block. DHCP Manager adds a list of contiguous addresses from this information. If you have several blocks of noncontiguous addresses, you can add the others by running DHCP Manager's Address Wizard again, after the initial configuration.

Before you configure your IP addresses, know how many addresses are in the initial block of addresses you want to add and the IP address of the first address in the range.

Client Host Name Generation

The dynamic nature of DHCP means that an IP address is not permanently associated with the host name of the system that is using it. The DHCP management tools can generate a client name to associate with each IP address if you select this option. The client names consist of a prefix, or root name, plus a dash and a number assigned by the server. For example, if the root name is `charlie`, the client names are `charlie-1`, `charlie-2`, `charlie-3`, and so on.

By default, generated client names begin with the name of the DHCP server that manages them. This strategy is useful in environments that have more than one DHCP server because you can quickly see in the DHCP network tables which clients any given DHCP server manages. However, you can change the root name to any name you choose.

Before you configure your IP addresses, decide if you want the DHCP management tools to generate client names, and if so, what root name to use for the names.

The generated client names can be mapped to IP addresses in `/etc/inet/hosts`, DNS, or NIS+ if you specify to register host names during DHCP configuration. See [“Client Host Name Registration” on page 308](#) for more information.

Default Client Configuration Macros

In Solaris DHCP, a *macro* is a collection of network configuration options and their assigned values. The DHCP server uses macros to determine what network configuration information to send to a DHCP client.

When you configure the DHCP server, the management tools gather information from system files and directly from you through prompts or command-line options you specify. With this information, the management tools create the following macros:

- **Network address macro** — The network address macro is named to match the IP address of the client network. For example, if the network is 192.68.0.0, the network address macro is also named 192.68.0.0. The macro contains information needed by any client that is part of the network, such as subnet mask, network broadcast address, default router or router discovery token, and NIS/NIS+ domain and server if the server uses NIS/NIS+. Other options that are applicable to your network might be included. The network address macro is automatically processed for all clients located on that network, as described in [“Order of Macro Processing” on page 260](#).
- **Locale macro** — The locale macro is named `Locale`. The macro contains the offset (in seconds) from Coordinated Universal Time (UTC) to specify the time zone. The locale macro is not automatically processed, but is included in the server macro.
- **Server macro** — The server macro is named to match the server’s host name. For example, if the server is named `pineola`, the server macro is also named `pineola`. The server macro contains information about the lease policy, time server, DNS domain, and DNS server, and possibly other information that the configuration program was able to obtain from system files. The server macro includes the locale macro, so the DHCP server processes the locale macro as part of the server macro.

When you configure IP addresses for the first network, you must select a client configuration macro to be used for all DHCP clients that use the addresses you are configuring. The macro that you select is mapped to the IP addresses. By default, the server macro is selected because the macro contains information needed by all clients that use this server.

Clients receive the options contained in the network address macro before the options in the macro that is mapped to IP addresses. This processing order causes the options in the server macro to take precedence over any conflicting options in the network address macro. See [“Order of Macro Processing” on page 260](#) for more information about the order in which macros are processed.

Dynamic and Permanent Lease Types

The *lease type* determines whether the lease policy applies to the IP addresses you are configuring. During initial server configuration, DHCP Manager allows you to select either dynamic or permanent leases for the addresses you are adding. If you configure the DHCP server with the `dhcpconfig` command, leases are dynamic.

When an IP address has a *dynamic lease*, the DHCP server can manage the address. The DHCP server can allocate the IP address to a client, extend the lease time, detect when the address is no longer in use, and reclaim the address. When an IP address has a *permanent lease*, the DHCP server can only allocate the address. The client then owns

the address until explicitly releasing the address. When the address is released, the server can assign the address to another client. The address is not subject to the lease policy as long as the address is configured with a permanent lease type.

When you configure a range of IP addresses, the lease type you select applies to all the addresses in the range. To get the most benefit from DHCP, you should use dynamic leases for most of the addresses. You can later modify individual addresses to make them permanent, if necessary. However, the total number of permanent leases should be kept to a minimum.

Reserved IP Addresses and Lease Type

IP addresses can be reserved by manually assigning them to particular clients. A reserved address can be associated with a permanent lease or a dynamic lease. When a reserved address is assigned a permanent lease, the following statements are true:

- The address can be allocated only to the client that is bound to the address.
- The DHCP server cannot allocate the address to another client.
- The address cannot be reclaimed by the DHCP server.

If a reserved address is assigned a dynamic lease, the address can be allocated only to the client that is bound to the address. However, the client must track lease time and negotiate for a lease extension as if the address were not reserved. This strategy enables you to track when the client is using the address by looking at the network table.

You cannot create reserved addresses for all the IP addresses during the initial configuration. Reserved addresses are intended to be used sparingly for individual addresses.

Planning for Multiple DHCP Servers

If you want to configure more than one DHCP server to manage your IP addresses, consider the following guidelines:

- Divide the pool of IP addresses so that each server is responsible for a range of addresses, and there is no overlap of responsibility.
- Choose NIS+ as your data store, if available. If not, choose text files and specify a shared directory for the absolute path to the data store. The binary files data store cannot be shared.
- Configure each server separately so that address ownership is allocated correctly and so that server-based macros can be automatically created.

- Set up the servers to scan the options and macros in the `dhcptab` table at specified intervals so that the servers are using the latest information. You can use DHCP Manager to schedule automatic reading of `dhcptab` as described in “Customizing Performance Options for the DHCP Server” on page 309.
- Be sure all clients can access all DHCP servers so that the servers can support one another. A client that has a valid IP address lease might try to verify its configuration or extend the lease when the server that owns the client’s address is not reachable. Another server can respond to the client after the client has attempted to contact the primary server for 20 seconds. If a client requests a specific IP address, and the server that owns the address is not available, one of the other servers handles the request. In this case, the client does not receive the requested address. The client receives an IP address that is owned by the responding DHCP server.

Planning DHCP Configuration of Your Remote Networks

After the initial DHCP configuration, you can place IP addresses in remote networks under DHCP management. However, because the system files are not local to the server, DHCP Manager and `dhcpconfig` cannot look up information to provide default values, so you must provide the information. Before you try to configure a remote network, be sure you know the following information:

- The remote network’s IP address.
- The subnet mask of the remote network. This information can be obtained from the `netmasks` table in the name service. If the network uses local files, look in `/etc/netmasks` on a system in the network. If the network uses NIS+, use the command `niscat netmasks.org_dir`. If the network uses NIS, use the command `ypcat -k netmasks.byaddr`. Make sure the `netmasks` table contains all the topology information for all the subnets you want to manage.
- The network type. The clients connect to the network through either a local area network (LAN) connection or a Point-to-Point Protocol (PPP).
- Routing information. Can the clients use router discovery? If not, you must determine the IP address of a router they can use.
- NIS domain and NIS servers, if applicable.
- NIS+ domain and NIS+ servers, if applicable.

See “Adding DHCP Networks” on page 314 for the procedure for adding DHCP networks.

Selecting the Tool for Configuring DHCP

After you gather information and plan for DHCP service, you are ready to configure a DHCP server. You can use the DHCP Manager or the command-line utility `dhcpconfig` to configure a server. DHCP Manager lets you select options and specify data that is then used to create the `dhcptab` and network tables used by the DHCP server. The `dhcpconfig` utility requires you to use command-line options to specify data.

DHCP Manager Features

DHCP Manager, a Java™ technology-based GUI tool, provides a DHCP Configuration Wizard. The configuration wizard starts automatically the first time you run DHCP Manager on a system that is not configured as a DHCP server. The DHCP Configuration Wizard provides a series of dialog boxes that prompt you for the essential information required to configure a server: data store format, lease policy, DNS/NIS/NIS+ servers and domains, and router addresses. Some of the information is obtained by the wizard from system files, and you only need to confirm that the information is correct, or to correct information, if necessary.

When you progress through the dialog boxes and approve the information, the DHCP server daemon starts on the server system. You are then prompted to start the Add Addresses Wizard to configure IP addresses for the network. Only the server's network is configured for DHCP initially, and other server options are given default values. You can run DHCP Manager again after the initial configuration is complete to add networks and modify other server options.

See [“Configuring and Unconfiguring a DHCP Server Using DHCP Manager” on page 279](#) for more information about the DHCP Configuration Wizard. See [“About DHCP Manager” on page 292](#) for more detailed information about DHCP Manager.

`dhcpconfig` Features

The `dhcpconfig` utility supports options that enable you to configure and unconfigure a DHCP server, as well as convert to a new data store and import/export data to and from other DHCP servers. When you use the `dhcpconfig` utility to configure a DHCP server, the utility obtains information from the system files discussed in [“Updating System Files and Netmask Tables” on page 266](#). You cannot view and confirm the information obtained from system files as you can with DHCP Manager. So, it is important that the system files be updated before you run `dhcpconfig`. You can also use command-line options to override the values `dhcpconfig` would obtain by default from system files. The `dhcpconfig` command can be used in scripts. See the `dhcpconfig(1M)` man page for more information.

Comparison of DHCP Manager and `dhcpconfig`

The following table summarizes the differences between the two server configuration tools.

TABLE 12-4 Comparison of DHCP Manager and the `dhcpconfig` Command

Feature	DHCP Manager	<code>dhcpconfig</code> With Options
Network information that is gathered from system.	Enables you to view the information gathered from system files, and to change it if needed.	You can specify the network information with command-line options.
Speed of configuration.	Speeds the configuration process by omitting prompts for nonessential server options, using default values instead. You can change nonessential options after initial configuration.	Fastest configuration process, but you might need to specify values for many options.

[Chapter 13](#) includes procedures you can use to configure your server with either DHCP Manager or the `dhcpconfig` utility.

Configuring the DHCP Service (Tasks)

When you configure the DHCP service on your network, you configure and start the first DHCP server. Other DHCP servers can be added later and can access the same data from a shared location if the data store supports shared data. This chapter describes tasks that enable you to configure the DHCP server and place networks and their associated IP addresses under DHCP management. This chapter also explains how to unconfigure a DHCP server.

Each task includes a procedure to help you perform the task in DHCP Manager and a procedure for the equivalent task with the `dhcpcfg` utility. This chapter contains the following information:

- “Configuring and Unconfiguring a DHCP Server Using DHCP Manager” on page 279
- “Configuring and Unconfiguring a DHCP Server Using `dhcpcfg` Commands” on page 287

If you experience problems configuring the DHCP service, see [Chapter 16](#).

After you configure the DHCP service, see [Chapter 14](#) for information about managing the DHCP service.

Configuring and Unconfiguring a DHCP Server Using DHCP Manager

This section includes procedures to help you configure and unconfigure a DHCP server with DHCP Manager. Note that you must be running an X Window system such as CDE or GNOME to use DHCP Manager.

DHCP Manager can be run as superuser with the `/usr/sadm/admin/bin/dhcpmgr` command. See “About DHCP Manager” on page 292 for general information about the utility. See “How to Start and Stop DHCP Manager” on page 294 for more detailed information about running DHCP Manager.

When you run DHCP Manager on a server that is not configured for DHCP, the following screen is displayed. You can specify whether you want to configure a DHCP server or a BOOTP relay agent.

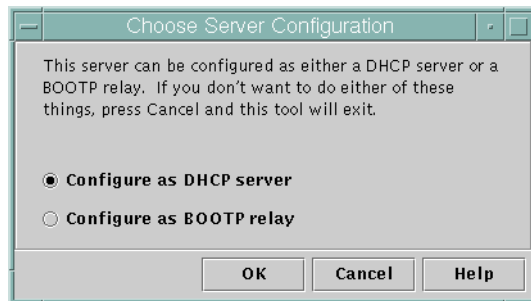


FIGURE 13-1 Choose Server Configuration Dialog Box in DHCP Manager

Configuring DHCP Servers

When you configure a DHCP server, DHCP Manager starts the DHCP Configuration Wizard, which prompts you for information that is needed to configure the server. The initial screen of the wizard is shown in the following figure.

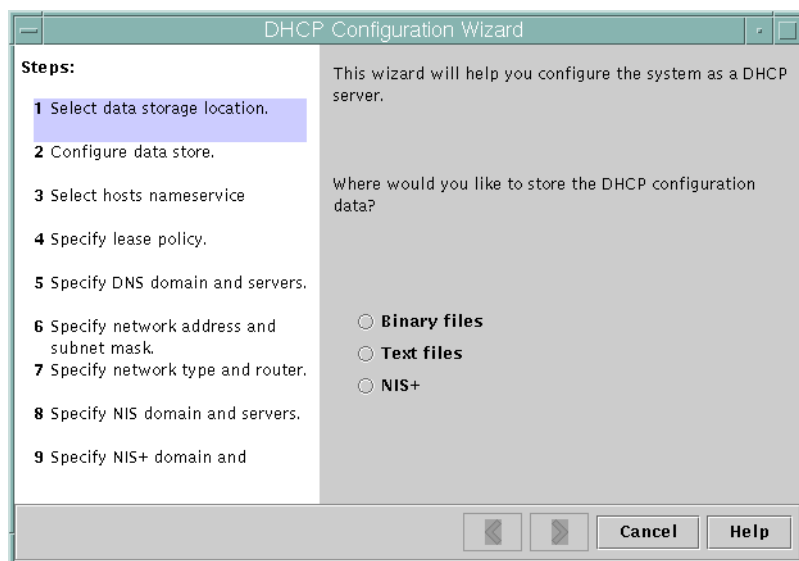


FIGURE 13-2 DHCP Configuration Wizard’s Initial Screen

When you finish answering the wizard prompts, DHCP Manager creates the items that are listed in the following table.

TABLE 13-1 Items Created During DHCP Server Configuration

Item	Description	Contents
Service configuration file, <code>/etc/inet/dhcpsvc.conf</code>	Records keywords and values for server configuration options.	Data store type and location, and options that are used with <code>in.dhcpd</code> to start the DHCP daemon when the system boots. Do not edit this file manually. You must use <code>dhcpmgr</code> or <code>dhcpconfig</code> to modify DHCP configuration information.
<code>dhcptab</code> table	DHCP Manager creates a <code>dhcptab</code> table if the table does not already exist.	Macros and options with assigned values.
Locale macro (optional), which is named <code>Locale</code>	Contains the local time zone’s offset in seconds from Universal time (UTC).	<code>UTCoffset</code> option with assigned number of seconds.

TABLE 13-1 Items Created During DHCP Server Configuration *(Continued)*

Item	Description	Contents
Server macro, which is named to match the server's node name	Contains options whose values are determined by input from the administrator who configured the DHCP server. Options apply to all clients that use addresses owned by the server.	The <code>Locale</code> macro, plus the following options: <ul style="list-style-type: none"> ■ <code>Timeserv</code>, set to point to the server's primary IP address. ■ <code>LeaseTim</code>, set to the number of seconds for the leases. ■ <code>LeaseNeg</code>, if you selected negotiable leases. ■ <code>DNSdmain</code> and <code>DNSserv</code>, if DNS is configured. ■ <code>Hostname</code>, which <i>must not</i> be assigned a value. The presence of this option indicates that the host name must be obtained from the name service.
Network address macro, whose name is the same as the network address of client's network	Contains options whose values are determined by input from the administrator who configured the DHCP server. Options apply to all clients that reside on the network specified by the macro name.	The following options: <ul style="list-style-type: none"> ■ <code>Subnet</code>, set to the subnet mask for the local subnet ■ <code>Router</code>, set to the IP address of a router, or <code>RdiscvyF</code>, to cause the client to use router discovery ■ <code>Broadcst</code>, set to the broadcast IP address. This option is present only if the network is not a Point-to-Point network. ■ <code>MTU</code>, for the maximum transmission unit ■ <code>NISdmain</code> and <code>NISservs</code>, if NIS is configured ■ <code>NIS+dom</code> and <code>NIS+serv</code>, if NIS+ is configured
Network table for the network	An empty table is created until you create IP addresses for the network.	No content until you add IP addresses.

▼ How to Configure a DHCP Server (DHCP Manager)

Before You Begin Make sure that you have read [Chapter 12](#) before you configure your DHCP server. In particular, you should use the guidelines in [“Making Decisions for Your DHCP Server Configuration \(Task Map\)”](#) on page 268 to help you perform the following tasks:

- Select the system that you want to use as a DHCP server.
- Make decisions about your data store, lease policy, and router information.

- Steps**
- 1. Become superuser on the server system.**
 - 2. Start DHCP Manager.**

```
#/usr/sadm/admin/bin/dhccpmgr &
```
 - 3. Choose the option Configure as DHCP Server.**
The DHCP Configuration Wizard starts, to help you configure your server.
 - 4. Select options, or type requested information, based on the decisions you made in the planning phase.**
If you have difficulty, click Help in the wizard window to open your web browser and display help for the DHCP Configuration Wizard.
 - 5. Click Finish to complete the server configuration when you have finished specifying the requested information.**
 - 6. At the Start Address Wizard prompt, click Yes to configure IP addresses for the server.**
The Add Addresses to Network wizard enables you to specify which addresses to place under the control of DHCP.
 - 7. Answer the prompts according to decisions you made in the planning phase.**
See [“Making Decisions for IP Address Management \(Task Map\)”](#) on page 271 for more information. If you have difficulty, click Help in the wizard window to open your web browser and display help for the Add Addresses to Network wizard.
 - 8. Review your selections, and then click Finish to add the IP addresses to the network table.**
The network table is updated with records for each address in the range you specified.

See Also You can add more networks to the DHCP server with the Network Wizard, as explained in [“Adding DHCP Networks”](#) on page 314.

Configuring BOOTP Relay Agents

When you configure a BOOTP relay agent, DHCP Manager takes the following actions:

- Prompts you for the IP address for one or more DHCP servers to which requests should be relayed
- Stores settings needed for BOOTP relay service

The following figure shows the screen displayed when you choose to configure a BOOTP relay agent.

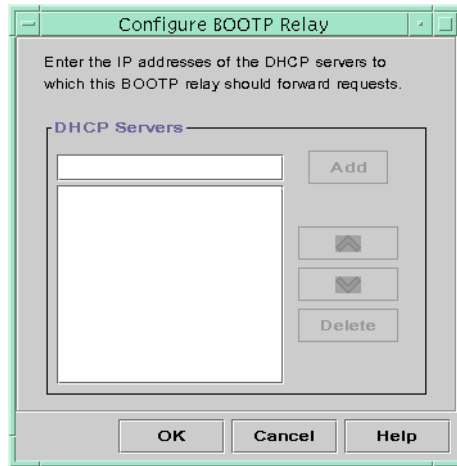


FIGURE 13-3 Configure BOOTP Relay Dialog Box in DHCP Manager

▼ How to Configure a BOOTP Relay Agent (DHCP Manager)

Before You Begin

Make sure that you have read [Chapter 12](#) before you configure your BOOTP relay agent. In particular, you should see “[Selecting a Host to Run the DHCP Service](#)” on [page 268](#) for help in selecting the system to use.

Steps

1. **Become superuser on the server system.**
2. **Start the DHCP Manager.**

```
#/usr/sadm/admin/bin/dhcpmgr &
```

If the system has not been configured as a DHCP server or BOOTP relay agent, the DHCP Configuration Wizard starts. If the system has already been configured as a DHCP server, you must first unconfigure the server. See “[Unconfiguring DHCP Servers and BOOTP Relay Agents](#)” on [page 285](#).

3. **Select Configure as BOOTP Relay.**
The Configure BOOTP Relay dialog box opens.
4. **Type the IP address or host name of one or more DHCP servers, and click Add.**
The specified DHCP servers must be configured to handle BOOTP or DHCP requests received by this BOOTP relay agent.
5. **Click OK to exit the dialog box.**

Notice that DHCP Manager offers only the File menu to exit the application and the Service menu to manage the server. The disabled menu options are useful only on a DHCP server.

Unconfiguring DHCP Servers and BOOTP Relay Agents

When you unconfigure a DHCP server or a BOOTP relay agent, DHCP Manager takes the following actions:

- Stops the DHCP daemon (`in.dhcpd`) process
- Removes the `/etc/inet/dhcpsvc.conf` file, which records information about daemon startup and the data store location

The following figure shows the screen that is displayed when you choose to unconfigure a DHCP server.

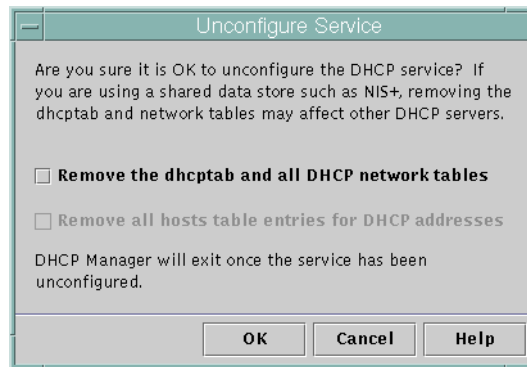


FIGURE 13-4 Unconfigure Service Dialog Box in DHCP Manager

DHCP Data on an Unconfigured Server

When you unconfigure a DHCP server, you must decide what to do with the `dhcptab` table and the DHCP network tables. If the data is shared among servers, you should not remove the `dhcptab` and DHCP network tables. If the tables are removed, DHCP would become unusable across your network. Data can be shared through NIS+ or on exported local file systems. The file `/etc/inet/dhcpsvc.conf` records the data store used and its location.

You can unconfigure a DHCP server but leave the data intact by not selecting any of the options to remove data. If you unconfigure the server and leave the data intact, you disable the DHCP server.

If you want another DHCP server to take ownership of the IP addresses, you must move the DHCP data to the other DHCP server. You must move the data before you unconfigure the current server. See [“Moving Configuration Data Between DHCP Servers \(Task Map\)”](#) on page 365 for more information.

If you are certain you want to remove the data, you can select an option to remove the `dhcptab` and network tables. If you had generated client names for the DHCP addresses, you can also elect to remove those entries from the hosts table. Client name entries can be removed from DNS, `/etc/inet/hosts`, or NIS+.

Before you unconfigure a BOOTP relay agent, be sure that no clients rely on this agent to forward requests to a DHCP server.

▼ How to Unconfigure a DHCP Server or a BOOTP Relay Agent (DHCP Manager)

Steps 1. Become superuser.

2. Start DHCP Manager.

```
#/usr/sadm/admin/bin/dhcpmgr &
```

3. From the Service menu, choose Unconfigure.

The Unconfigure Service dialog box is displayed. If the server is a BOOTP relay agent, the dialog box enables you to confirm your intention to unconfigure the relay agent. If the server is a DHCP server, you must decide what to do with the DHCP data and make selections in the dialog box. See [Figure 13–4](#).

4. (Optional) Select options to remove data.

If the server uses shared data through NIS+ or in files shared through NFS, do not select any options to remove the data. If the server does not use shared data, select one option or both options to remove the data.

See [“DHCP Data on an Unconfigured Server”](#) on page 285 for more information about removing data.

5. Click OK to unconfigure the server.

The Unconfigure Service dialog box and DHCP Manager are closed.

Configuring and Unconfiguring a DHCP Server Using `dhcpcfg` Commands

This section includes procedures to help you configure and unconfigure a DHCP server or a BOOTP relay agent by using `dhcpcfg` with command-line options.

▼ How to Configure a DHCP Server (`dhcpcfg -D`)

Before You Begin

Make sure that you have read [Chapter 12](#) before you configure your DHCP server. In particular, you should use the guidelines in “[Making Decisions for Your DHCP Server Configuration \(Task Map\)](#)” on page 268 to help you perform the following tasks:

- Select the system that you want to use as a DHCP server.
- Make decisions about your data store, lease policy, and router information.

Steps

1. **Log in to the system on which you want to configure the DHCP server.**
2. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**

For more information about the DHCP Management profile, see “[Setting Up User Access to DHCP Commands](#)” on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see “[Configuring RBAC \(Task Map\)](#)” in *System Administration Guide: Security Services*.

3. **Configure the DHCP server by typing a command of the following format:**

```
#/usr/sbin/dhcpcfg -D -r datastore -p location
```

datastore is one of the following: `SUNWfiles`, `SUNWbinfiles`, or `SUNWnisplus`.

location is the data-store-dependent location where you want to store the DHCP data. For `SUNWfiles` and `SUNWbinfiles`, the location must be an absolute path name. For `SUNWnisplus`, the location must be a fully specified NIS+ directory.

For example, you might type a command similar to the following:

```
dhcpcfg -D -r SUNWbinfiles -p /var/dhcp
```

The `dhcpcfg` utility uses the host’s system files and network files to determine values used to configure the DHCP server. See the `dhcpcfg(1M)` man page for information about additional options to the `dhcpcfg` command that enable you to override the default values.

4. **Add one or more networks to the DHCP service.**

See “How to Add a DHCP Network (`dhcpcfg`)” on page 316 for the procedure to add a network.

▼ How to Configure a BOOTP Relay Agent (`dhcpcfg -R`)

Before You Begin Select the system that you want to use as a BOOTP relay agent, using the requirements listed in “Selecting a Host to Run the DHCP Service” on page 268.

- Steps**
1. **Log in to the server that you want to configure as a BOOTP relay agent.**
 2. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see “Setting Up User Access to DHCP Commands” on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.
 3. **Configure the BOOTP relay agent by typing a command of the following format:**

```
# /usr/sbin/dhcpcfg -R server-addresses
```

Specify one or more IP addresses of DHCP servers to which you want requests to be forwarded. If you specify more than one address, separate the addresses with commas.

For example, you might type a command similar to the following:

```
/usr/sbin/dhcpcfg -R 192.168.1.18,192.168.42.132
```

▼ How to Unconfigure a DHCP Server or a BOOTP Relay Agent (`dhcpcfg -U`)

- Steps**
1. **Log in to the DHCP server or the BOOTP relay agent system that you want to unconfigure.**
 2. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see “Setting Up User Access to DHCP Commands” on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

3. Unconfigure the DHCP server or the BOOTP relay agent:

```
# /usr/sbin/dhcpconfig -U
```

If the server does not use shared data, you can also use the `-x` option to remove the `dhcptab` and network tables. If the server uses shared data, do not use the `-x` option. The `-h` option can be used to remove host names from the host table. See the `dhcpconfig(1M)` man page for more information about `dhcpconfig` options. See [“DHCP Data on an Unconfigured Server” on page 285](#) for more information about removing data.

Administering DHCP (Tasks)

This chapter describes tasks that you might find useful when you administer the Solaris DHCP service. The chapter includes tasks for the server, BOOTP relay agent, and client. Each task includes a procedure to help you perform the task in DHCP Manager and a procedure for the equivalent task with DHCP command-line utilities. DHCP command-line utilities are more fully documented in man pages.

You should have already completed the initial configuration of your DHCP service and initial network before you use this chapter. [Chapter 13](#) discusses DHCP configuration.

This chapter contains the following information:

- “About DHCP Manager” on page 292
- “Setting Up User Access to DHCP Commands” on page 295
- “Starting and Stopping the DHCP Service” on page 296
- “DHCP Service and the Service Management Facility” on page 298
- “Modifying DHCP Service Options (Task Map)” on page 299
- “Adding, Modifying, and Removing DHCP Networks (Task Map)” on page 311
- “Supporting BOOTP Clients With the DHCP Service (Task Map)” on page 321
- “Working With IP Addresses in the DHCP Service (Task Map)” on page 324
- “Working With DHCP Macros (Task Map)” on page 340
- “Working With DHCP Options (Task Map)” on page 350
- “Supporting Solaris Network Installation With the DHCP Service” on page 360
- “Supporting Remote Boot and Diskless Boot Clients (Task Map)” on page 361
- “Setting Up DHCP Clients to Receive Information Only (Task Map)” on page 362
- “Converting to a New DHCP Data Store” on page 363
- “Moving Configuration Data Between DHCP Servers (Task Map)” on page 365

About DHCP Manager

DHCP Manager is a graphical user interface (GUI) tool that you can use to perform administration tasks on the DHCP service.

DHCP Manager Window

The DHCP Manager window's appearance depends on how the DHCP server is configured on the system on which DHCP Manager is running.

DHCP Manager uses a tab-based window when the system is configured as a DHCP server. You select a tab for the type of information you want to work with. DHCP Manager features the following tabs:

- **Addressestab** – Lists all networks and IP addresses placed under DHCP management. From the Addresses tab, you can work with networks and IP addresses. You can add or delete items individually or in blocks. You can also modify the properties of individual networks or IP addresses or simultaneously make the same property modifications for a block of addresses. When you start DHCP Manager, the Addresses tab opens first.
- **Macros** tab – Lists all available macros in the DHCP configuration table (`dhcptab`) and the options contained within the macros. From the Macros tab, you can create or delete macros. You can also modify macros by adding options and providing values for the options.
- **Options** tab – Lists all options that have been defined for this DHCP server. Options that are listed on this tab are not the standard options defined in the DHCP protocol. The options are extensions to the standard options, and have a class of Extended, Vendor, or Site. Standard options cannot be changed in any way so those options are not listed here.

The following figure shows how the DHCP Manager window might look when you start DHCP Manager on a DHCP server.

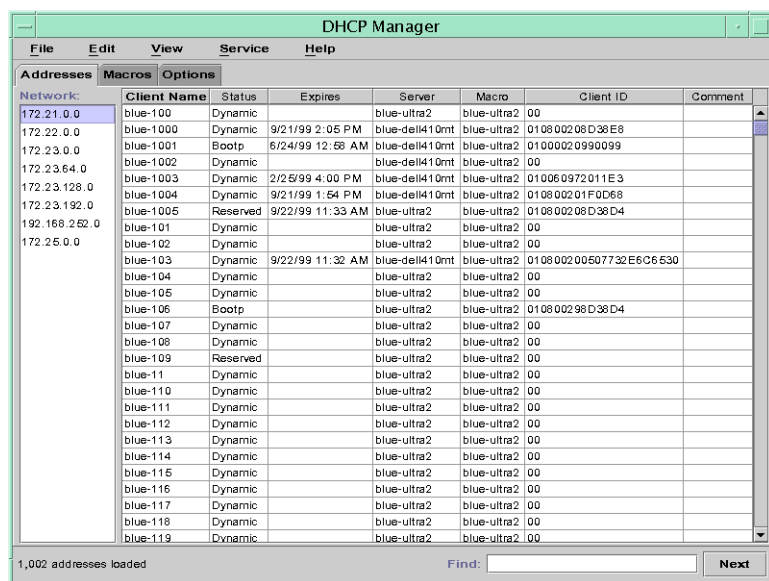


FIGURE 14-1 DHCP Manager on a DHCP Server System

When the server is configured as a BOOTP relay agent, the DHCP Manager window does not show these tabs. The BOOTP relay agent does not need the same information. You can only modify the BOOTP relay agent's properties and stop or start the DHCP daemon with DHCP Manager. The following figure shows how DHCP Manager might look on a system that is configured as a BOOTP relay agent.

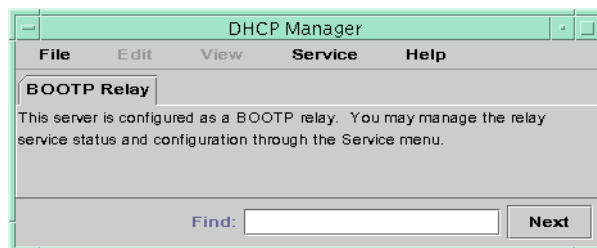


FIGURE 14-2 DHCP Manager on a BOOTP Relay Agent

DHCP Manager Menus

DHCP Manager menus include the following items:

- **File** – Exit DHCP Manager.
- **Edit** – Perform management tasks for networks, addresses, macros, and options.

- **View** – Change the look of the tab currently selected.
- **Service** – Manage the DHCP daemon and data store.
- **Help** – Open your web browser and display help for DHCP Manager.

When DHCP Manager runs on a BOOTP relay agent, the Edit and View menus are disabled.

All DHCP management tasks are accomplished through the Edit and Service menus.

You use the commands in the Edit menu to create, delete, and modify items in the selected tab. Items can include networks, addresses, macros, and options. When the Addresses tab is selected, the Edit menu also lists wizards. Wizards are sets of dialogs that help you create networks and multiple IP addresses.

The Service menu lists commands that enable you to manage the DHCP daemon. From the Service menu, you can perform the following tasks:

- Start and stop the DHCP daemon.
- Enable and disable the DHCP daemon.
- Modify the server configuration.
- Unconfigure the server.
- Convert the data store.
- Export and import data on the server.

Starting and Stopping DHCP Manager

You must run DHCP Manager on a DHCP server system as superuser. If you must run DHCP Manager remotely, you can send the display to your system by using the X Window remote display feature.

▼ How to Start and Stop DHCP Manager

- Steps**
1. **Become superuser on the DHCP server system.**
 2. **(Optional) If you are logged in to the DHCP server system remotely, display DHCP Manager on your local system as follows.**
 - a. **Type the following on the local system:**

```
# xhost +server-name
```
 - b. **Type the following on the remote DHCP server system:**

```
# DISPLAY=local-hostname;export DISPLAY
```
 3. **Start DHCP Manager.**

```
# /usr/sadm/admin/bin/dhcppmgr &
```

The DHCP Manager window opens. If the server is configured as a DHCP server, the window displays the Addresses tab. If the server is configured as a BOOTP relay agent, the window displays with no tabs.

4. To stop DHCP Manager, choose Exit from the File menu.

The DHCP Manager window closes.

Setting Up User Access to DHCP Commands

By default, only root or superuser can execute `dhcpconfig`, `dhtadm`, and `pntadm` commands. If you want non-root users to use the commands, you can set up role-based access control (RBAC) for those commands.

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

You might also find the following man pages helpful: `rbac(5)`, `exec_attr(4)`, and `user_attr(4)`.

The following procedure explains how to assign the DHCP Management profile, which enables the user to execute the DHCP commands.

▼ How to Grant Users Access to DHCP Commands

- Steps**
- 1. Become superuser on the DHCP server system.**
 - 2. Edit the file `/etc/user_attr` to add an entry of the following form. Add one entry for each user or role that should manage the DHCP service.**

```
username:::type=normal;profiles=DHCP Management
```

For example, for user `ram`, you would add the following entry:

```
ram:::type=normal;profiles=DHCP Management
```

Starting and Stopping the DHCP Service

This section describes starting and stopping the DHCP service by using DHCP Manager and the `dhcpconfig` command. The DHCP service can also be started and stopped by using the Service Management Facility (SMF) commands. See “[DHCP Service and the Service Management Facility](#)” on page 298 for more information about using SMF commands with the DHCP service.

Starting and stopping the DHCP service encompasses several degrees of action you can take to affect the operation of the DHCP daemon. You must understand what each action means in order to select the correct procedure to obtain the result that you want. The terms for the actions are as follows:

- **Start, stop, and restart commands** affect the daemon only for the current session. For example, if you stop the DHCP service, the daemon terminates but restarts when you reboot the system. DHCP data tables are not affected when you stop the service. You can use DHCP Manager or SMF commands to temporarily start and stop the DHCP service without enabling and disabling the service.
- **Enable and disable commands** affect the daemon for current and future sessions. If you disable the DHCP service, the currently running daemon terminates and does not start when you reboot the server. You must enable the DHCP daemon for automatic startup at system boot to occur. DHCP data tables are not affected. You can use DHCP Manager, the `dhcpconfig` command, or SMF commands to enable and disable the DHCP service.
- The **unconfigure command** shuts down the daemon, prevents the daemon from starting on system reboot, and enables you to remove the DHCP data tables. You can use DHCP Manager or the `dhcpconfig` command to unconfigure the DHCP service. Unconfiguration is described in [Chapter 13](#).

Note – If a server has multiple network interfaces but you do not want to provide DHCP services on all the networks, see “[Specifying Network Interfaces for DHCP Monitoring](#)” on page 312.

The following procedures help you start, stop, enable, and disable the DHCP service.

▼ How to Start and Stop the DHCP Service (DHCP Manager)

Steps 1. Become superuser on the DHCP server system.

2. Start DHCP Manager.

```
# /usr/sadm/admin/bin/dhcpmgr &
```

3. Select one of the following:

- Choose Start from the Service menu to start the DHCP service.
- Choose Stop from the Service menu to stop the DHCP service.
The DHCP daemon stops until it is restarted, or the system reboots.
- Choose Restart from the Service menu to stop and immediately restart the DHCP service.

▼ How to Enable and Disable the DHCP Service (DHCP Manager)

Step ● In DHCP Manager, choose one of the following:

- Choose Enable from the Service menu to configure the DHCP daemon for automatic startup when the system boots.
The DHCP service starts immediately when it is enabled.
- Choose Disable from the Service menu to prevent the DHCP daemon from automatically starting when the system boots.
The DHCP service immediately stops when it is disabled.

▼ How to Enable and Disable the DHCP Service (dhcpconfig -S)

Steps 1. Log in to the DHCP server system.

2. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

3. Choose one of the following:

- To enable the DHCP service, type the following command:

```
# /usr/sbin/dhcpconfig -S -e
```

- To disable the DHCP service, type the following command:

```
# /usr/sbin/dhcpconfig -S -d
```

DHCP Service and the Service Management Facility

The Service Management Facility (SMF) is described in Chapter 9, “Managing Services (Overview),” in *System Administration Guide: Basic Administration*. The SMF `svcadm` command can be used to enable and start the DHCP server, and disable and stop the DHCP server. However, you cannot use SMF commands to modify the DHCP service options that the DHCP tools allow you to set. In particular, service options that are stored in the `/etc/dhcp/dhcpd.conf` file cannot be set by using the SMF tools.

The following table maps DHCP commands to the equivalent SMF commands.

TABLE 14-1 SMF Commands For DHCP Server Tasks

Task	DHCP Command	SMF Command
Enable DHCP service	<code>dhcpconfig -S -e</code>	<code>svcadm enable</code> <code>svc:/network/dhcp-server</code>
Disable DHCP service	<code>dhcpconfig -S -d</code>	<code>svcadm disable</code> <code>svc:/network/dhcp-server</code>
Start DHCP service for current session only	None	<code>svcadm enable -t</code> <code>svc:/network/dhcp-server</code>
Stop DHCP service for current session	None	<code>svcadm disable -t</code> <code>svc:/network/dhcp-server</code>

TABLE 14-1 SMF Commands For DHCP Server Tasks (Continued)

Task	DHCP Command	SMF Command
Restart DHCP service	<code>dhcpcfg -S -r</code>	<code>svcadm restart</code> <code>svc:/network/dhcp-server</code>

Modifying DHCP Service Options (Task Map)

You can change values for some additional features of the DHCP service, which might not have been offered during the initial configuration with DHCP Manager. To change service options, you can use the Modify Service Options dialog box in DHCP Manager. Or you can specify options with the `dhcpcfg` command.

The following task map shows the tasks related to service options and the procedures to use.

Task	Description	For Instructions
Change logging options.	Enable or disable logging, and select a <code>syslog</code> facility to use for logging DHCP transactions.	<p>“How to Generate Verbose DHCP Log Messages (DHCP Manager)” on page 302</p> <p>“How to Generate Verbose DHCP Log Messages (Command Line)” on page 303</p> <p>“How to Enable and Disable DHCP Transaction Logging (DHCP Manager)” on page 303</p> <p>“How to Enable and Disable DHCP Transaction Logging (Command Line)” on page 304</p> <p>“How to Log DHCP Transactions to a Separate <code>syslog</code> File” on page 305</p>
Change DNS update options.	Enable or disable server’s capability to dynamically add DNS entries for clients that supply a host name. Determine the maximum time the server should spend attempting to update DNS.	<p>“How to Enable Dynamic DNS Updating for DHCP Clients” on page 306</p>

Task	Description	For Instructions
Enable or disable duplicate IP address detection.	Enable or disable the DHCP server's capability to determine that an IP address is not already in use before offering the address to a client.	"How to Customize DHCP Performance Options (DHCP Manager)" on page 310 "How to Customize DHCP Performance Options (Command Line)" on page 310
Change options for the DHCP server's reading of configuration information.	Enable or disable the automatic reading of <code>dhcpcd.conf</code> at specified intervals, or change the interval between reads.	"How to Customize DHCP Performance Options (DHCP Manager)" on page 310 "How to Customize DHCP Performance Options (Command Line)" on page 310
Change the number of relay agent hops.	Increase or decrease the number of networks a request can travel through before being dropped by the DHCP daemon.	"How to Customize DHCP Performance Options (DHCP Manager)" on page 310 "How to Customize DHCP Performance Options (Command Line)" on page 310
Change the length of time an IP address offer is cached.	Increase or decrease the number of seconds that the DHCP service reserves an offered IP address before offering the address to a new client.	"How to Customize DHCP Performance Options (DHCP Manager)" on page 310 "How to Customize DHCP Performance Options (Command Line)" on page 310

The following figure shows DHCP Manager's Modify Service Options dialog box.

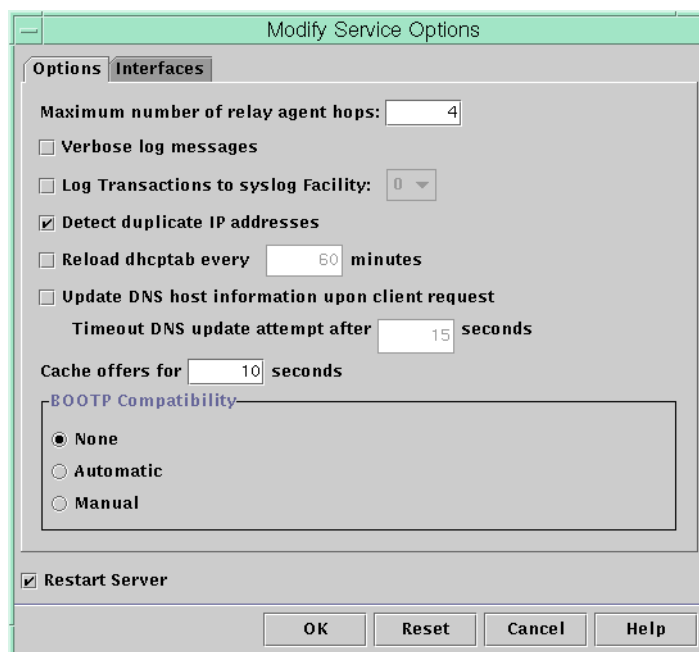


FIGURE 14-3 Modify Service Options Dialog Box in DHCP Manager

Changing DHCP Logging Options

The DHCP service can log DHCP service messages and DHCP transactions to `syslog`. See the `syslogd(1M)` and `syslog.conf(4)` man pages for more information about `syslog`.

DHCP service messages logged to `syslog` include the following:

- Error messages, which notify you of conditions that prevent the DHCP service from fulfilling a request by a client or by you.
- Warnings and notices, which notify you of conditions that are abnormal, but do not prevent the DHCP service from fulfilling a request.

You can increase the amount of information that is reported by using the verbose option for the DHCP daemon. Verbose message output can help you troubleshoot DHCP problems. See “[How to Generate Verbose DHCP Log Messages \(DHCP Manager\)](#)” on page 302.

Another useful troubleshooting technique is transaction logging. Transactions provide information about every interchange between a DHCP server or BOOTP relay and clients. DHCP transactions include the following message types:

- ASSIGN – IP address assignment
- ACK – Server acknowledges that the client accepts the offered IP address, and sends configuration parameters
- EXTEND – Lease extension
- RELEASE – IP address release
- DECLINE – Client is declining address assignment
- INFORM – Client is requesting network configuration parameters but not an IP address
- NAK – Server does not acknowledge a client’s request to use a previously used IP address
- ICMP_ECHO – Server detects potential IP address is already in use by another host

BOOTP relay transactions include the following message types:

- RELAY-CLNT – Message is being relayed from the DHCP client to a DHCP server
- RELAY-SRV – Message is being relayed from the DHCP server to the DHCP client

DHCP transaction logging is disabled by default. When enabled, DHCP transaction logging uses the `local0` facility in `syslog` by default. DHCP transaction messages are generated with a `syslog` severity level of *notice*. This security level causes DHCP transactions to be logged to the file where other system notices are logged. However, because the `local` facility is used, the DHCP transaction messages can be logged separately from other notices. To log the transaction messages separately, you must edit the `syslog.conf` file to specify a separate log file. See the `syslog.conf(4)` man page for more information about the `syslog.conf` file.

You can disable or enable transaction logging, and you can specify a different `syslog` facility, from `local0` through `local7`, as explained in [“How to Enable and Disable DHCP Transaction Logging \(DHCP Manager\)”](#) on page 303. In the server system’s `syslog.conf` file, you can also instruct `syslogd` to store the DHCP transaction messages in a separate file. See [“How to Log DHCP Transactions to a Separate `syslog` File”](#) on page 305 for more information.

▼ How to Generate Verbose DHCP Log Messages (DHCP Manager)

Steps 1. In DHCP Manager, choose **Modify from the Service menu**.

See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.

The Modify Service Options dialog box opens and displays the Options tab. See [Figure 14-3](#).

2. Select Verbose Log Messages.

3. Select Restart Server.

The Restart Server option is near the bottom of the dialog box.

4. Click OK.

The daemon runs in verbose mode for this session and each subsequent session until you reset this option. Verbose mode can reduce daemon efficiency because of the time that is taken to display messages.

▼ How to Generate Verbose DHCP Log Messages (Command Line)

Steps 1. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)” in *System Administration Guide: Security Services*](#).

2. Type the following command to set verbose mode:

```
# /usr/sbin/dhcpconfig -P VERBOSE=true
```

The next time the DHCP server starts, the server runs in verbose mode until you turn off verbose mode.

To turn off verbose mode, type the following command:

```
# /usr/sbin/dhcpconfig -P VERBOSE=
```

This command sets the VERBOSE keyword to no value, which causes the keyword to be removed from the server’s configuration file.

Verbose mode can reduce daemon efficiency because of the time that is taken to display messages.

▼ How to Enable and Disable DHCP Transaction Logging (DHCP Manager)

This procedure enables and disables transaction logging for all subsequent DHCP server sessions.

- Steps**
1. **In DHCP Manager, choose Modify from the Service menu.**
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 2. **Select Log Transactions to Syslog Facility.**
To disable transaction logging, deselect this option.
 3. **(Optional) Select a local facility from 0 to 7 to use for logging DHCP transactions.**
By default, DHCP transactions are logged to the location where system notices are logged, which depends on how `syslogd` is configured. If you want the DHCP transactions to be logged to a file separate from other system notices, see [“How to Log DHCP Transactions to a Separate syslog File” on page 305](#).
Message files can quickly become very large when transaction logging is enabled.
 4. **Select Restart Server.**
 5. **Click OK.**
The daemon logs transactions to the selected `syslog` facility for this session and each subsequent session until you disable logging.

▼ How to Enable and Disable DHCP Transaction Logging (Command Line)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)” in *System Administration Guide: Security Services*](#).
 2. **Choose one of the following steps:**
 - **To enable DHCP transaction logging, type the following command:**

```
# /usr/sbin/dhcpconfig -P LOGGING_FACILITY=syslog-local-facility
```

`syslog-local-facility` is a number from 0 through 7. If you omit this option, 0 is used.
By default, DHCP transactions are logged to the location where system notices are logged, which depends on how `syslogd` is configured. If you want the DHCP transactions to be logged to a file separate from other system notices, see [“How to Log DHCP Transactions to a Separate syslog File” on page 305](#).
Message files can quickly become very large when transaction logging is enabled.

- To disable DHCP transaction logging, type the following command:

```
# /usr/sbin/dhcpconfig -P LOGGING_FACILITY=
```

Note that you supply no value for the parameter.

▼ How to Log DHCP Transactions to a Separate syslog File

- Steps**
1. **Become superuser or assume an equivalent role on the DHCP server system.**

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

A role that is assigned to the DHCP Management profile might not be sufficient for this task. The role must have permission to edit syslog files.

2. **Edit the `/etc/syslog.conf` file on the server system to add a line of the following format:**

```
localn.notice    path-to-logfile
```

n is the syslog facility number you specified for transaction logging, and *path-to-logfile* is the complete path to the file to use for logging transactions.

For example, you might add the following line:

```
local0.notice /var/log/dhcpdsvc
```

See the `syslog.conf(4)` man page for more information about the `syslog.conf` file.

Enabling Dynamic DNS Updates by a DHCP Server

DNS provides name-to-address and address-to-name services for the Internet. Once a DNS mapping is made, a system can be reached through its host name or its IP address. The system is also reachable from outside its domain.

The DHCP service can use DNS in two ways:

- The DHCP server can look up the host name that is mapped to an IP address that the server is assigning to the client. The server then returns the client's host name along with the client's other configuration information.
- The DHCP server can attempt to make a DNS mapping on a client's behalf, if the DHCP server is configured to update DNS. The client can supply its own host name when requesting DHCP service. If configured to make DNS updates, the DHCP server attempts to update DNS with the client's suggested host name. If the DNS update is successful, the DHCP server returns the requested host name to the client. If the DNS update is not successful, the DHCP server returns a different host name to the client.

You can enable the DHCP service to update the DNS service for DHCP clients that supply their own host names. For the DNS update feature to work, the DNS server, the DHCP server, and the DHCP client must be set up correctly. In addition, the requested host name must not be in use by another system in the domain.

The DHCP server's DNS update feature works if the following statements are true:

- The DNS server supports RFC 2136.
- The DNS software is based on BIND v8.2.2, patch level 5 or later, whether on the DHCP server system or the DNS server system.
- The DNS server is configured to accept dynamic DNS updates from the DHCP server.
- The DHCP server is configured to make dynamic DNS updates.
- DNS support is configured for the DHCP client's network on the DHCP server.
- The DHCP client is configured to supply a requested host name in its DHCP request message.
- The requested host name corresponds to a DHCP-owned address. The host name could also have no corresponding address.

▼ How to Enable Dynamic DNS Updating for DHCP Clients

Note – Be aware that dynamic DNS updates are a *security risk*.

By default, the Solaris DNS daemon (`in.named`) does not allow dynamic updates. Authorization for dynamic DNS updates is granted in the `named.conf` configuration file on the DNS server system. No other security is provided. You must carefully weigh the convenience of this facility for users against the security risk created when you enable dynamic DNS updates.

- Steps**
1. On the DNS server, edit the `/etc/named.conf` file as superuser.
 2. Find the zone section for the appropriate domain in the `named.conf` file.
 3. Add the DHCP server's IP addresses to the `allow-update` keyword.

If the `allow-update` keyword does not exist, insert the keyword.

For example, if the DHCP server resides at addresses `10.0.0.1` and `10.0.0.2`, a `named.conf` file for the `dhcp.domain.com` zone should be modified as follows:

```
zone "dhcp.domain.com" in {
    type master;
    file "db.dhcp";
    allow-update { 10.0.0.1; 10.0.0.2; };
};

zone "10.IN-ADDR.ARPA" in {
    type master;
    file "db.10";
    allow-update { 10.0.0.1; 10.0.0.2; };
};
```

Note that `allow-update` for both zones must be enabled to allow the DHCP server to update both A and PTR records on the DNS server.

4. On the DHCP server, start DHCP Manager.

```
# /usr/sadm/admin/bin/dhcpmgr &
```

See [“How to Start and Stop DHCP Manager”](#) on page 294 for more detailed information.

5. Choose **Modify** from the **Service** menu.

The **Modify Service Options** dialog box opens.

6. Select **Update DNS Host Information Upon Client Request**.

7. Specify the number of seconds to wait for a response from the DNS server before timing out, then click **OK**.

The default value of 15 seconds should be adequate. If you have timeout problems, you can increase the value later.

8. Click the **Macros** tab, and ensure that the correct DNS domain is specified.

The `DNSdomain` option must be passed with the correct domain name to any client that expects dynamic DNS update support. By default, `DNSdomain` is specified in the server macro, which is used as the configuration macro bound to each IP address.

9. Set up the DHCP client to specify its host name when requesting DHCP service.

If you use the Solaris DHCP client, see [“How to Enable a Solaris Client to Request a Specific Host Name”](#) on page 380. If your client is not a Solaris DHCP client, see the documentation for your DHCP client for information about how to specify a host name.

Client Host Name Registration

If you let the DHCP server generate host names for the IP addresses that you place in the DHCP service, the DHCP server can register those host names in NIS+, `/etc/inet/hosts`, or DNS name services. Host name registration cannot be done in NIS because NIS does not provide a protocol to allow programs to update and propagate NIS maps.

Note – The DHCP server can update DNS with generated host names only if the DNS server and the DHCP server are running on the same system.

If a DHCP client provides its host name and the DNS server is configured to allow dynamic updates from the DHCP server, the DHCP server can update DNS on the client's behalf. Dynamic updates can be done even if the DNS and DHCP servers are running on different systems. See [“Enabling Dynamic DNS Updates by a DHCP Server” on page 305](#) for more information about enabling this feature.

The following table summarizes client host name registration for DHCP client systems with the various name services.

TABLE 14-2 Client Host Name Registration in Name Services

Name Service	Who Registers Host Name	
	DHCP-Generated Host Name	DHCP Client-Supplied Host Name
NIS	NIS Administrator	NIS Administrator
NIS+	DHCP tools	DHCP tools
<code>/etc/hosts</code>	DHCP tools	DHCP tools
DNS	DHCP tools, if the DNS server runs on the same system as the DHCP server DNS Administrator, if the DNS server runs on a different system	DHCP server, if configured for dynamic DNS updates DNS Administrator, if DHCP server is not configured for dynamic DNS updates

Solaris DHCP clients can request particular host names in DHCP requests if configured to do so as described in [“How to Enable a Solaris Client to Request a Specific Host Name” on page 380](#). Refer to the vendor documentation for other DHCP clients to determine if the capability is supported.

Customizing Performance Options for the DHCP Server

You can change options that affect the performance of the DHCP server. These options are described in the following table.

TABLE 14-3 Options Affecting DHCP Server Performance

Server Option	Description	Keyword
Maximum number of BOOTP relay agent hops	If a request has traveled through more than a given number of BOOTP relay agents, the request is dropped. The default maximum number of relay agent hops is four. This number is likely to be sufficient for most networks. A network might need more than four hops if DHCP requests pass through several BOOTP relay agents before reaching a DHCP server.	RELAY_HOPS= <i>integer</i>
Detect duplicate addresses	By default, the server pings an IP address before offering the address to a client. A lack of response to the ping verifies that the address is not already in use. You can disable this feature to decrease the time that the server takes to make an offer. However, disabling the feature creates the risk of having duplicate IP addresses in use.	ICMP_VERIFY=TRUE/FALSE
Reload <code>dhcptab</code> automatically at specified intervals	The server can be set to automatically read the <code>dhcptab</code> at the interval, in minutes, that you specify. If your network configuration information does not change frequently, and you do not have multiple DHCP servers, you do not need to reload the <code>dhcptab</code> automatically. Also, note that DHCP Manager gives you the option to have the server reload the <code>dhcptab</code> after you make a change to the data.	RESCAN_INTERVAL= <i>min</i>
Cache offers of IP addresses for specified intervals	After a server offers an IP address to a client, the offer is cached. While the offer is cached, the server does not offer the address again. You can change the number of seconds for which the offer is cached. The default is 10 seconds. On slow networks, you might need to increase the offer time.	OFFER_CACHE_TIMEOUT= <i>sec</i>

The following procedures describe how to change these options.

▼ How to Customize DHCP Performance Options (DHCP Manager)

- Steps**
1. In DHCP Manager, choose **Modify** from the **Service** menu.
See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.
 2. **Change the desired options.**
See [Table 14-3](#) for information about the options.
 3. **Select Restart Server.**
 4. **Click OK.**

▼ How to Customize DHCP Performance Options (Command Line)

If you change options with this procedure, the changed options are used only after the DHCP server is restarted.

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

2. **Modify one or more performance options:**

```
# /usr/sbin/dhccpconfig -P keyword=value,keyword=value...
```

keyword=value can be any of the following keywords:

RELAY_HOPS=*integer*

Specifies the maximum number of relay agent hops that can occur before the daemon drops the DHCP or BOOTP datagram.

ICMP_VERIFY=TRUE/FALSE

Enables or disables automatic duplicate IP address detection. Setting this keyword to FALSE is not recommended.

RESCAN_INTERVAL=*minutes*

Specifies the interval in minutes that the DHCP server should use to schedule the automatic rereading of the `dhcptab` information.

OFFER_CACHE_TIMEOUT=*seconds*

Specifies the number of seconds the DHCP server should cache the offers that are extended to discovering DHCP clients. The default setting is 10 seconds.

Example 14–1 Setting DHCP Performance Options

The following is an example of how to specify all the command options.

```
# dhcpconfig -P RELAY_HOPS=2,ICMP_VERIFY=TRUE,\nRESCAN_INTERVAL=30,OFFER_CACHE_TIMEOUT=20
```

Adding, Modifying, and Removing DHCP Networks (Task Map)

When you configure a DHCP server, you must also configure at least one network in order to use the DHCP service. You can add more networks at any time.

The following task map lists tasks that you can perform when working with DHCP networks. The task map includes links to procedures for carrying out the tasks.

Task	Description	For Instructions
Enable or disable the DHCP service on server network interfaces	The default behavior is to monitor all network interfaces for DHCP requests. If you do not want all interfaces to accept DHCP requests, you can remove an interface from the list of monitored interfaces.	“How to Specify Network Interfaces for DHCP Monitoring (DHCP Manager)” on page 313
Add a new network to the DHCP service.	Places a network under DHCP management, for the purpose of managing IP addresses on the network.	“How to Add a DHCP Network (DHCP Manager)” on page 315 “How to Add a DHCP Network (dhcpconfig)” on page 316
Change parameters of a DHCP-managed network.	Modifies the information that is passed to clients of a particular network.	“How to Modify the Configuration of a DHCP Network (DHCP Manager)” on page 317 “How to Modify the Configuration of a DHCP Network (dhtadm)” on page 318

Task	Description	For Instructions
Delete a network from the DHCP service.	Removes a network so that IP addresses on the network are no longer managed by DHCP.	“How to Remove a DHCP Network (DHCP Manager)” on page 320 “How to Remove a DHCP Network (pnt adm)” on page 320

Specifying Network Interfaces for DHCP Monitoring

By default, both `dhcpconfig` and DHCP Manager’s Configuration Wizard configure the DHCP server to monitor all the server system’s network interfaces. If you add a new network interface to the server system, the DHCP server automatically monitors the new interface when you boot the system. You can then add any networks to be monitored through the network interface.

However, you can also specify which network interfaces should be monitored, and which interfaces should be ignored. You might want to ignore an interface if you do not want to offer DHCP service on that network.

If you specify that any interface should be ignored, and then install a new interface, the DHCP server ignores the new interface. You must add the new interface to the server’s list of monitored interfaces. You can specify interfaces with DHCP Manager or the `dhcpconfig` utility.

This section includes procedures that enable you to specify which network interfaces DHCP should monitor or ignore. The DHCP Manager procedure uses the Interfaces tab of the DHCP Manager’s Modify Service Options dialog box, which is shown in the following figure.

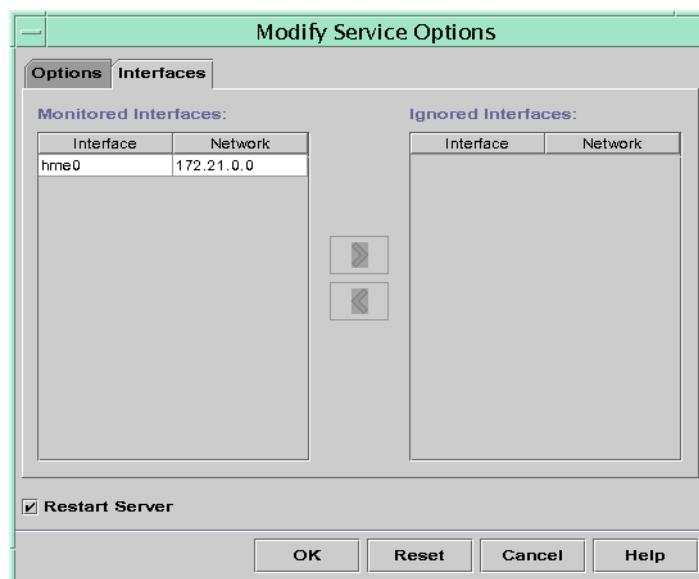


FIGURE 14-4 Interfaces Tab of Modify Service Options Dialog Box in DHCP Manager

▼ How to Specify Network Interfaces for DHCP Monitoring (DHCP Manager)

- Steps**
1. **In DHCP Manager, choose Modify from the Service menu.**
The Modify Service Options dialog box is displayed.
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 2. **Select the Interfaces tab.**
 3. **Select the appropriate network interface.**
 4. **Click the arrow buttons to move the interface to the appropriate list.**
For example, to ignore an interface, select the interface in the Monitored Interfaces list, and then click the right arrow button. The interface is then shown in the Ignored Interfaces list.
 5. **Select Restart Server, and click OK.**
The changes you make persist across reboots.

▼ How to Specify Network Interfaces for DHCP Monitoring (`dhcpconfig`)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

2. **Type the following command on the DHCP server system:**

```
# /usr/sbin/dhcpconfig -P INTERFACES=int,int,...
```

`int, int,...` is a list of interfaces to monitor. The interface names must be separated by commas.

For example, you would use the following command to monitor only `ge0` and `ge1`:

```
#/usr/sbin/dhcpconfig -P INTERFACES=ge0,ge1
```

Interfaces that you want to ignore should be omitted from the `dhcpconfig` command line.

The changes you make with this command persist across reboots.

Adding DHCP Networks

When you use DHCP Manager to configure the server, the first network is also configured at the same time. The first network is usually the local network on the server system’s primary interface. If you want to configure additional networks, use the DHCP Network Wizard in DHCP Manager.

If you use the `dhcpconfig -D` command to configure the server, you must separately configure all networks that you want to use the DHCP service. See [“How to Add a DHCP Network \(`dhcpconfig`\)”](#) on page 316 for more information.

The following figure shows the initial dialog box for the DHCP Network Wizard in DHCP Manager.

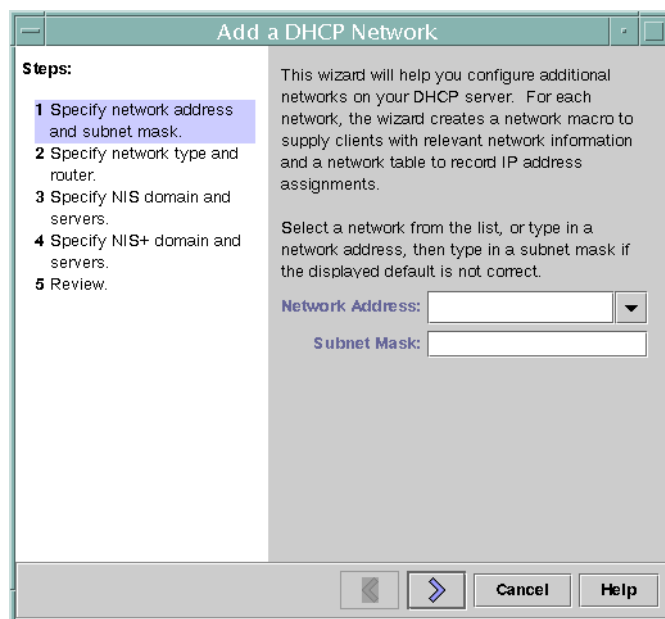


FIGURE 14-5 DHCP Manager’s Network Wizard

When you configure a new network, DHCP Manager creates the following components:

- A network table in the data store. The new network is shown in the network list within the Addresses tab of DHCP Manager.
- A network macro that contains information needed by clients that reside on this network. The network macro’s name matches the IP address of the network. The network macro is added to the `dhcptab` table in the data store.

▼ How to Add a DHCP Network (DHCP Manager)

- Steps**
1. **In DHCP Manager, click the Addresses tab.**
Any networks already configured for DHCP service are listed.
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 2. **Choose Network Wizard from the Edit menu.**
 3. **Select options, or type requested information. Use the decisions that you made during the planning phase to determine what information to specify.**
Planning is described in [“Planning DHCP Configuration of Your Remote Networks” on page 275](#).

If you have difficulty with the wizard, click Help in the wizard window. Your web browser displays help for the DHCP Network Wizard.

4. Click Finish to complete the network configuration when you have finished specifying the requested information.

The Network Wizard creates an empty network table, which is listed in the left pane of the window.

The Network Wizard also creates a network macro whose name matches the IP address of the network.

5. (Optional) Select the Macros tab and select the network macro to view the macro's contents.

You can confirm that the information that you provided in the wizard has been inserted as values for options in the network macro.

See Also You must add addresses for the network before the network's IP addresses can be managed under DHCP. See ["Adding IP Addresses to the DHCP Service"](#) on page 328 for more information.

If you leave the network table empty, the DHCP server can still provide configuration information to clients. See ["Setting Up DHCP Clients to Receive Information Only \(Task Map\)"](#) on page 362 for more information.

▼ How to Add a DHCP Network (dhcpconfig)

Steps **1. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**

For more information about the DHCP Management profile, see ["Setting Up User Access to DHCP Commands"](#) on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see ["Configuring RBAC \(Task Map\)"](#) in *System Administration Guide: Security Services*.

2. Type the following command on the DHCP server system:

```
# /usr/sbin/dhcpconfig -N network-address
```

network-address is the IP address of the network you want to add to the DHCP service. See the dhcpconfig(1M) man page for suboptions you can use with the -N option.

If you do not use suboptions, dhcpconfig uses network files to obtain information about the network.

See Also You must add addresses for the network before the network's IP addresses can be managed under DHCP. See ["Adding IP Addresses to the DHCP Service"](#) on page 328 for more information.

If you leave the network table empty, the DHCP server can still provide configuration information to clients. See [“Setting Up DHCP Clients to Receive Information Only \(Task Map\)”](#) on page 362 for more information.

Modifying DHCP Network Configurations

After you add a network to the DHCP service, you can modify the configuration information that you originally supplied. The configuration information is stored in the network macro used to pass information to clients on the network. You must modify the network macro to change the network configuration.

The following figure shows the Macros tab of DHCP Manager.

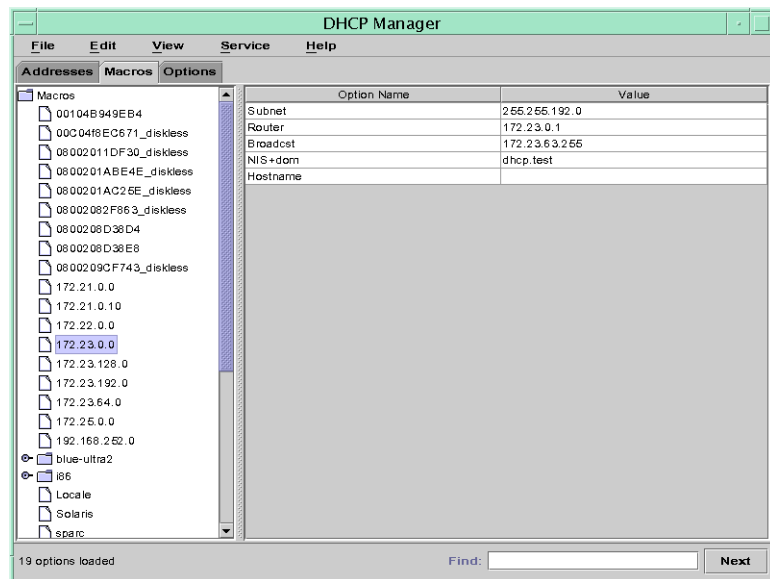


FIGURE 14-6 DHCP Manager’s Macros Tab

▼ How to Modify the Configuration of a DHCP Network (DHCP Manager)

Steps 1. In DHCP Manager, select the Macros tab.

All macros that are defined for this DHCP server are listed in the left pane.

See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.

2. **Select the network macro whose name matches the network configuration that you are changing.**
The network macro name is the network IP address.
3. **Choose Properties from the Edit menu.**
The Macro Properties dialog box displays a table of the options included in the macro.
4. **Select the option that you want to modify.**
The option name and its value are displayed in text fields near the top of the dialog box.
5. **(Optional) Modify the option name, or choose the Select button to display a list of option names.**
The Select Option dialog box displays a list of all DHCP standard options, with a brief description of each option.
6. **(Optional) Select an option name in the Select Option dialog box, and click OK.**
The new option name is displayed in the Option Name field.
7. **Type the new value for the option, and click Modify.**
8. **(Optional) You can also add options to the network macro by choosing Select in the dialog box.**
See [“Modifying DHCP Macros” on page 342](#) for more general information about modifying macros.
9. **Select Notify DHCP Server of Change, and click OK.**
This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.

▼ How to Modify the Configuration of a DHCP Network (`dhtadm`)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.
 2. **Determine which macro includes information for all clients of the network.**
The network macro’s name matches the network IP address.

If you don't know which macro includes this information, you can display the `dhcptab` table to list all macros by using the command `dhtadm -P`.

3. **Type a command of the following format to change the value of the option you want to change:**

```
# dhtadm -M -m macro-name -e 'symbol=value' -g
```

See the `dhtadm(1M)` man page for more information about `dhtadm` command-line options.

Example 14–2 Using the `dhtadm` Command to Modify a DHCP Macro

For example, to change the `10.25.62.0` macro's lease time to 57600 seconds and the NIS domain to `sem.example.com`, you would type the following commands:

```
# dhtadm -M -m 10.25.62.0 -e 'LeaseTim=57600' -g
```

```
# dhtadm -M -m 10.25.62.0 -e 'NISdomain=sem.example.com' -g
```

The `-g` option causes the DHCP daemon to reread the `dhcptab` table and put the changes into effect.

Removing DHCP Networks

DHCP Manager enables you to remove multiple networks at once. You have the option to automatically remove the hosts table entries associated with the DHCP-managed IP addresses on those networks as well. The following figure shows DHCP Manager's Delete Networks dialog box.

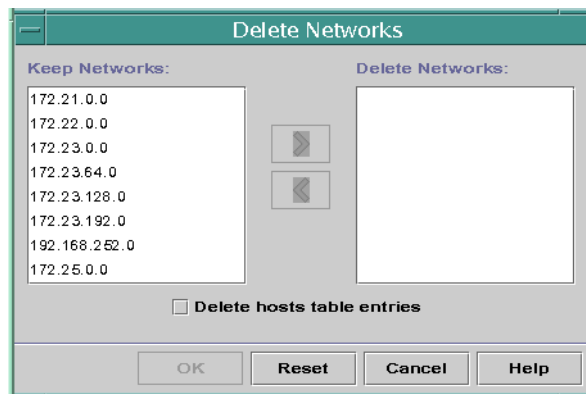


FIGURE 14–7 Delete Networks Dialog Box in DHCP Manager

The `pntadm` command requires you to delete each IP address entry from a network before you delete that network. You can delete only one network at a time.

▼ How to Remove a DHCP Network (DHCP Manager)

- Steps**
- 1. In DHCP Manager, select the Addresses tab.**
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 - 2. Choose Delete Networks from the Edit menu.**
The Delete Networks dialog box opens.
 - 3. In the Keep Networks list, select the networks that you want to delete.**
Press the Control key while you click with the mouse to select multiple networks.
Press the Shift key while you click to select a range of networks.
 - 4. Click the right arrow button to move the selected networks to the Delete Networks list.**
 - 5. If you want to remove the host table entries for this network’s DHCP addresses, select Delete Host Table Entries.**
Note that deleting host table entries does not delete the host registrations at the DNS server for these addresses. Entries are deleted only in the local name service.
 - 6. Click OK.**

▼ How to Remove a DHCP Network (pntadm)

Note that this procedure deletes the network’s IP addresses from the DHCP network table before removing the network. The addresses are deleted to ensure that the host names are removed from the `hosts` file or database.

- Steps**
- 1. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.
 - 2. Type a command following this format to remove an IP address and its host name from the name service:**

```
# pntadm -D -y IP-address
```


For example, to remove IP address 10.25.52.1, you would type the following command:


```
# pntadm -D -y 10.25.52.1
```

The `-y` option specifies to delete the host name.

3. Repeat the `pntadm -D -y` command for each address in the network.

You might want to create a script to run the `pntadm` command if you are deleting many addresses.

4. After all addresses are deleted, type the following command to delete the network from the DHCP service.

```
# pntadm -R network-IP-address
```

For example, to remove network `10.25.52.0`, you would type the following command:

```
# pntadm -R 10.25.52.0
```

See the `pntadm(1M)` man page for more information about using the `pntadm` utility.

Supporting BOOTP Clients With the DHCP Service (Task Map)

To support BOOTP clients on your DHCP server, you must set up your DHCP server to be BOOTP compatible. If you want to specify which BOOTP clients can use your DHCP, you can register BOOTP clients in the DHCP server's network table.

Alternatively, you can reserve a number of IP addresses for automatic allocation to BOOTP clients.

Note – BOOTP addresses are permanently assigned, whether or not you explicitly assign a permanent lease to the address.

The following task map lists tasks that you might need to perform to support BOOTP clients. The task map contains links to the procedures used to carry out the tasks.

Task	Description	For Instructions
Set up automatic BOOTP support.	Provides IP address for any BOOTP client on a DHCP-managed network, or on a network connected by a relay agent to a DHCP-managed network. You must reserve a pool of addresses for exclusive use by BOOTP clients. This option might be more useful if the server must support a large number of BOOTP clients.	“How to Set Up Support of Any BOOTP Client (DHCP Manager)” on page 322
Set up manual BOOTP support.	Provides IP address for only those BOOTP clients that have been manually registered with the DHCP service. This option requires you to bind a client’s ID to a particular IP address that has been marked for BOOTP clients. This option is useful for a small number of BOOTP clients, or when you want to restrict the BOOTP clients that can use the DHCP server.	“How to Set Up Support of Registered BOOTP Clients (DHCP Manager)” on page 323

▼ How to Set Up Support of Any BOOTP Client (DHCP Manager)

- Steps**
- 1. In DHCP Manager, select Modify from the Service menu.**
The Modify Service Options dialog box opens.
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 - 2. In the BOOTP Compatibility section of the dialog box, select Automatic.**
 - 3. Select Restart Server, and click OK.**
 - 4. Select the Addresses tab.**
 - 5. Select addresses that you want to reserve for BOOTP clients.**
Select a range of addresses by clicking the first address, pressing the Shift key, and clicking the last address. Select multiple nonconcurrent addresses by pressing the Control key while clicking each address.
 - 6. Select Properties from the Edit menu.**

The Modify Multiple Addresses dialog box opens.

7. **In the BOOTP section, select Assign All Addresses Only to BOOTP Clients.**
All other options should be set to Keep Current Settings.
8. **Click OK.**
Any BOOTP client can now obtain an address from this DHCP server.

▼ How to Set Up Support of Registered BOOTP Clients (DHCP Manager)

- Steps**
1. **In DHCP Manager, select Modify from the Service menu.**
The Modify Service Options dialog box opens.
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 2. **In the BOOTP Compatibility section of the dialog box, select Manual.**
 3. **Select Restart Server, and click OK.**
 4. **Select the Addresses tab.**
 5. **Select an address that you want to assign to a particular BOOTP client.**
 6. **Choose Properties from the Edit menu.**
The Address Properties dialog box opens.
 7. **In the Address Properties dialog box, select the Lease tab.**
 8. **In the Client ID field, type the client’s identifier.**
For a BOOTP Solaris client on an Ethernet network, the client ID is a string that is derived from the client’s hexadecimal Ethernet address. The client ID includes a prefix that indicates the Address Resolution Protocol (ARP) type for Ethernet (01). For example, a BOOTP client with the Ethernet address 8:0:20:94:12:1e would use the client ID 0108002094121E.

Tip – As superuser on a Solaris client system, type the following command to obtain the Ethernet address for the interface:

```
# ifconfig -a
```

9. **Select Reserved to reserve the IP address for this client.**
10. **Select Assign Only to BOOTP Clients, and click OK.**

In the Addresses tab, BOOTP is displayed in the Status field, and the client ID you specified is listed in the Client ID field.

Working With IP Addresses in the DHCP Service (Task Map)

You can use DHCP Manager or the `pntadm` command to add IP addresses, modify address properties, and remove addresses from the DHCP service. Before you work with IP addresses, you should refer to [Table 14-4](#) to become familiar with IP address properties. The table provides information for users of DHCP Manager and `pntadm`.

Note – [Table 14-4](#) includes examples of using `pntadm` to specify IP address properties while adding and modifying IP addresses. Refer also to the `pntadm(1M)` man page for more information about `pntadm`.

The following task map lists tasks that you must perform to add, modify, or remove IP addresses. The task map also contains links to the procedures used to carry out the tasks.

Task	Description	For Instructions
Add single or multiple IP addresses to the DHCP service.	Adds IP addresses on networks that are already managed by the DHCP service by using DHCP Manager.	“How to Add a Single IP Address (DHCP Manager)” on page 330 “How to Duplicate an Existing IP Address (DHCP Manager)” on page 330 “How to Add Multiple IP Addresses (DHCP Manager)” on page 331 “How to Add IP Addresses (pntadm)” on page 331
Change properties of an IP address.	Changes any of the IP address properties described in Table 14-4 .	“How to Modify IP Address Properties (DHCP Manager)” on page 333 “How to Modify IP Address Properties (pntadm)” on page 334

Task	Description	For Instructions
Remove IP addresses from the DHCP service.	Prevents the use of specified IP addresses by DHCP.	<p>“How to Mark IP Addresses as Unusable (DHCP Manager)” on page 335</p> <p>“How to Mark IP Addresses as Unusable (pnt adm)” on page 335</p> <p>“How to Delete IP Addresses From DHCP Service (DHCP Manager)” on page 336</p> <p>“How to Delete IP Addresses From the DHCP Service (pnt adm)” on page 337</p>
Assign a consistent IP address to a DHCP client.	Sets up a client to receive the same IP address each time the client requests its configuration.	<p>“How to Assign a Consistent IP Address to a DHCP Client (DHCP Manager)” on page 338</p> <p>“How to Assign a Consistent IP Address to a DHCP Client (pnt adm)” on page 339</p>

The following table lists and describes the properties of IP addresses.

TABLE 14-4 IP Address Properties

Property	Description	How to Specify in pnt adm Command
Network address	<p>The address of the network that contains the IP address that you are working with.</p> <p>The network address is displayed in the Networks list within the Addresses tab in DHCP Manager.</p>	<p>The network address must be the last argument on the pnt adm command line used to create, modify, or delete an IP address.</p> <p>For example, to add an IP address to network 10.21.0.0, you would type:</p> <pre>pntadm -A ip-address options 10.21.0.0</pre>
IP address	<p>The address you are working with, whether you are creating, modifying, or deleting the address.</p> <p>The IP address is displayed in the first column of the DHCP Manager’s Addresses tab.</p>	<p>The IP address must accompany the -A, -M, and -D options to the pnt adm command.</p> <p>For example, to modify IP address 10.21.5.12, you would type:</p> <pre>pntadm -M 10.21.5.12 options 10.21.0.0</pre>
Client name	<p>The host name mapped to the IP address in the hosts table. This name can be automatically generated by DHCP Manager when addresses are created. If you create a single address, you can supply the name.</p>	<p>Specify the client name with the -h option.</p> <p>For example, to specify client name carrot12 for 10.21.5.12, you would type:</p> <pre>pntadm -M 10.21.5.12 -h carrot12 10.21.0.0</pre>

TABLE 14-4 IP Address Properties (Continued)

Property	Description	How to Specify in <code>pntadm</code> Command
Owned by server	The DHCP server that manages the IP address and responds to the DHCP client's request for IP address allocation.	Specify the owning server name with the <code>-s</code> option. For example to specify server <code>blue2</code> to own address <code>10.21.5.12</code> , you would type: <code>pntadm -M 10.21.5.12 -s blue2 10.21.0.0</code>
Configuration macro	The macro that the DHCP server uses to obtain network configuration options from the <code>dhcptab</code> table. Several macros are created automatically when you configure a server, and when you add networks. See “About DHCP Macros” on page 259 for more information about macros. When addresses are created, a server macro is also created. The server macro is assigned as the configuration macro for each address.	Specify the macro name with the <code>-m</code> option. For example, to assign the server macro <code>blue2</code> to address <code>10.21.5.12</code> , you would type: <code>pntadm -M 10.21.5.12 -m blue2 10.21.0.0</code>
Client ID	A text string that is unique within the DHCP service. If the client ID is listed as <code>00</code> , the address is not allocated to any client. If you specify a client ID when modifying the properties of an IP address, the address is bound exclusively to that client. The client ID is determined by the vendor of the DHCP client. If your client is not a Solaris DHCP client, consult your DHCP client documentation for more information.	Specify the client ID with the <code>-i</code> option. For example, to assign client ID <code>08002094121E</code> to address <code>10.21.5.12</code> , you would type: <code>pntadm -M 10.21.5.12 -i 0108002094121E 10.21.0.0</code>

TABLE 14-4 IP Address Properties (Continued)

Property	Description	How to Specify in <code>pntadm</code> Command
	<p>For Solaris DHCP clients, the client ID is derived from the client's hexadecimal hardware address. The client ID includes a prefix that represents the ARP code for the type of network, such as 01 for Ethernet. The ARP codes are assigned by the Internet Assigned Numbers Authority (IANA) in the ARP Parameters section of the Assigned Numbers standard at http://www.iana.com/numbers.html</p> <p>For example, a Solaris client with the hexadecimal Ethernet address <code>8:0:20:94:12:1e</code> uses the client ID <code>0108002094121E</code>. The client ID is listed in DHCP Manager and <code>pntadm</code> when a client is currently using an address.</p> <p>Tip: As superuser on the Solaris client system, type the following command to obtain the Ethernet address for the interface: <code>ifconfig -a</code></p>	
Reserved	<p>The setting that specifies the address is reserved exclusively for the client indicated by the client ID, and the DHCP server cannot reclaim the address. If you choose this option, you manually assign the address to the client.</p>	<p>Specify that the address is reserved, or manual, with the <code>-f</code> option.</p> <p>For example, to specify that IP address <code>10.21.5.12</code> is reserved for a client, you would type:</p> <pre>pntadm -M 10.21.5.12 -f MANUAL 10.21.0.0</pre>
Lease type or policy	<p>The setting that determines how DHCP manages the use of IP addresses by clients. A lease is either dynamic or permanent. See “Dynamic and Permanent Lease Types” on page 273 for a complete explanation.</p>	<p>Specify that the address is permanently assigned with the <code>-f</code> option. Addresses are dynamically leased by default.</p> <p>For example, to specify that IP address <code>10.21.5.12</code> has a permanent lease, you would type:</p> <pre>pntadm -M 10.21.5.12 -f PERMANENT 10.21.0.0</pre>
Lease expiration date	<p>The date when the lease expires, applicable only when a dynamic lease is specified. The date is specified in <code>mm/dd/yyyy</code> format.</p>	<p>Specify a lease expiration date with the <code>-e</code> option.</p> <p>For example, to specify an expiration date of January 1, 2006, you would type:</p> <pre>pntadm -M 10.21.5.12 -e 01/01/2006 10.21.0.0</pre>

TABLE 14-4 IP Address Properties (Continued)

Property	Description	How to Specify in <code>pntadm</code> Command
BOOTP setting	The setting that marks the address as reserved for BOOTP clients. See “Supporting BOOTP Clients With the DHCP Service (Task Map)” on page 321 for more information about supporting BOOTP clients.	Reserve an address for BOOTP clients with the <code>-f</code> option. For example, to reserve IP address <code>10.21.5.12</code> for BOOTP clients, you would type: <code>pntadm -M 10.21.5.12 -f BOOTP 10.21.0.0</code>
Unusable setting	The setting that marks the address to prevent assignment of the address to any client.	Mark an address as unusable with the <code>-f</code> option. For example, to mark IP address <code>10.21.5.12</code> as unusable, you would type: <code>pntadm -M 10.21.5.12 -f UNUSABLE 10.21.0.0</code>

Adding IP Addresses to the DHCP Service

Before you add IP addresses, you must add the network that owns the addresses to the DHCP service. See [“Adding DHCP Networks”](#) on page 314 for information about adding networks.

You can add addresses with DHCP Manager or the `pntadm` command.

On networks that are already managed by the DHCP service, you can add addresses in several ways with DHCP Manager:

- **Add a single IP address** – Place one new IP address under DHCP management.
- **Duplicate an existing IP address** – Copy the properties of an existing IP address managed by DHCP, and supply a new IP address and client name.
- **Add a range of multiple IP addresses** – Use the Address Wizard to place a series of IP addresses under DHCP management.

The following figure shows the Create Address dialog box. The Duplicate Address dialog box is identical to the Create Address dialog box, except that the text fields display the values for an existing address.

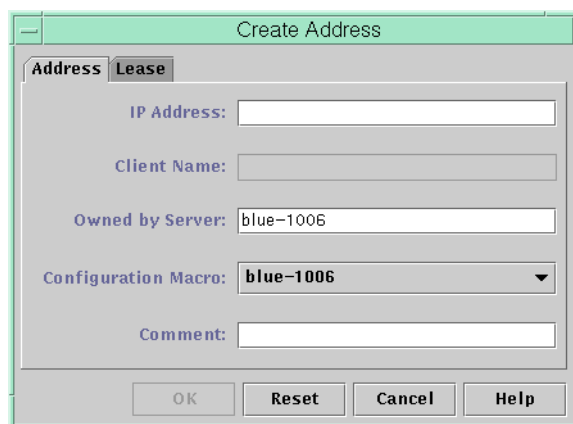


FIGURE 14-8 Create Address Dialog Box in DHCP Manager

The following figure shows the first dialog of the Add Addresses to Network wizard, used to add a range of IP addresses.

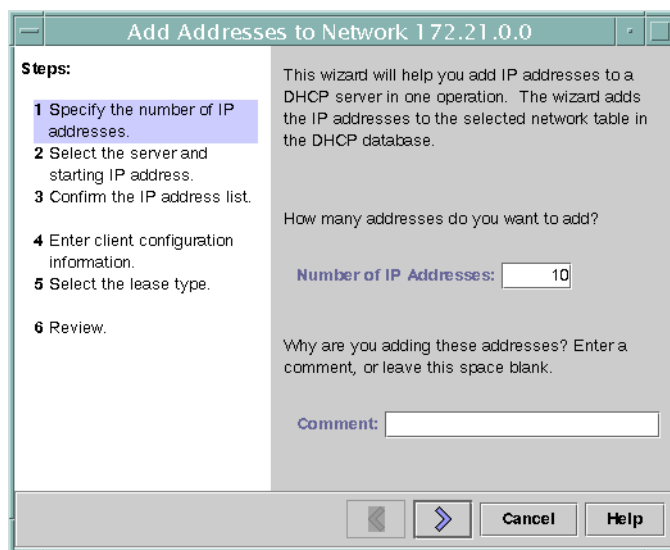


FIGURE 14-9 Add Addresses to Network Wizard in DHCP Manager

▼ How to Add a Single IP Address (DHCP Manager)

- Steps**
1. In DHCP Manager, select the **Addresses** tab.
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 2. Select the network where the new IP address is to be added.
 3. Choose **Create** from the **Edit** menu.
The Create Address dialog box opens.
 4. Select or type values for the address settings on the **Address** and **Lease** tabs.
Select the **Help** button to open a web browser to display help for the dialog box. Also, see [Table 14-4](#) for detailed information about the settings.
 5. Click **OK**.

▼ How to Duplicate an Existing IP Address (DHCP Manager)

- Steps**
1. In DHCP Manager, select the **Addresses** tab.
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 2. Select the network where the new IP address is located.
 3. Select the address with properties that you want to duplicate.
 4. Choose **Duplicate** from the **Edit** menu.
 5. Specify the new IP address in the **IP Address** field.
 6. (Optional) Specify a new client name for the address.
You cannot use the same name that is used by the address that you are duplicating.
 7. (Optional) Modify other option values, if necessary.
Most other option values should remain the same.
 8. Click **OK**.

▼ How to Add Multiple IP Addresses (DHCP Manager)

- Steps**
1. **In DHCP Manager, select the Addresses tab.**
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 2. **Select the network where the new IP addresses are to be added.**
 3. **Choose Address Wizard from the Edit menu.**
The Add Addresses to Network dialog box prompts you to provide values for the IP address properties. See [Table 14-4](#) for more information about the properties, or select the Help button in the dialog box. [“Making Decisions for IP Address Management \(Task Map\)” on page 271](#) includes more extensive information.
 4. **Click the right arrow button as you finish each screen, and click Finish on the last screen.**
The Addresses tab is updated with the new addresses.

▼ How to Add IP Addresses (pntadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)” in *System Administration Guide: Security Services*](#).
 2. **Add IP addresses by typing a command of the following format:**

```
# pntadm -A ip-address options network-address
```


Refer to the `pntadm(1M)` man page for a list of options you can use with `pntadm -A`. In addition, [Table 14-4](#) shows some sample `pntadm` commands that specify options.

Note – You can write a script to add multiple addresses with `pntadm`. See [Example 17-1](#) for an example.

Modifying IP Addresses in the DHCP Service

You can modify any of the address properties described in [Table 14-4](#) by using DHCP Manager or the `pntadm -M` command. See the `pntadm(1M)` man page for more information about `pntadm -M`.

The following figure shows the Address Properties dialog box that you use to modify IP address properties.

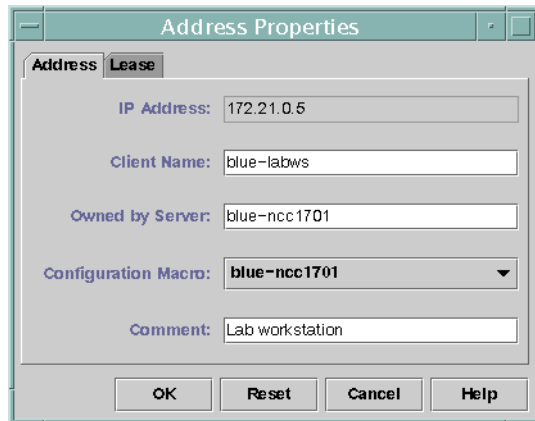


FIGURE 14-10 Address Properties Dialog Box in DHCP Manager

The following figure shows the Modify Multiple Addresses dialog box that you use to modify multiple IP addresses.

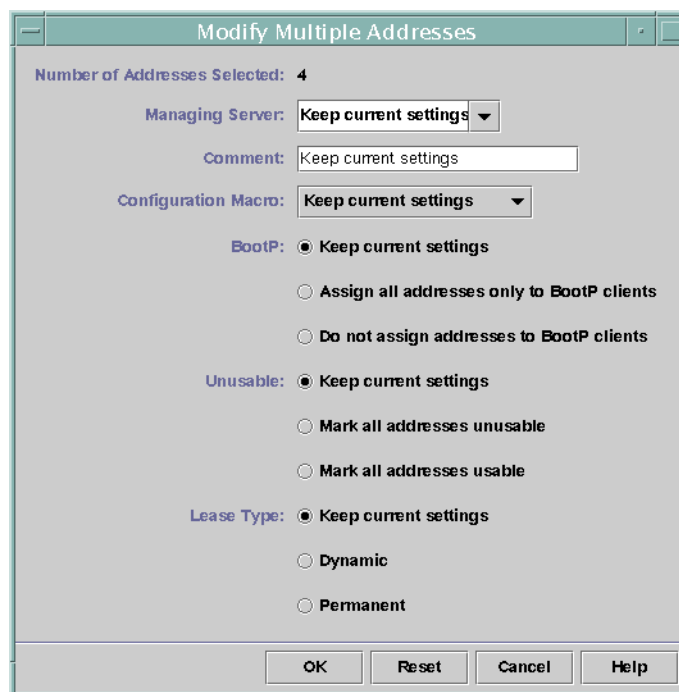


FIGURE 14-11 Modify Multiple Addresses Dialog Box in DHCP Manager

▼ How to Modify IP Address Properties (DHCP Manager)

- Steps**
1. **In DHCP Manager, select the Addresses tab.**
See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.
 2. **Select the IP address’s network.**
 3. **Select one or more IP addresses to modify.**
If you want to modify more than one address, press the Control key while you click with the mouse to select multiple addresses. You can also press the Shift key while you click to select a block of addresses.
 4. **Choose Properties from the Edit menu.**
The Address Properties dialog box or the Modify Multiple Address dialog box opens.
 5. **Change the appropriate properties.**

Click the Help button, or refer to [Table 14-4](#) for information about the properties.

6. Click OK.

▼ How to Modify IP Address Properties (pntadm)

Steps 1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

2. **Modify IP address properties by typing a command of the following format:**

```
# pntadm -M ip-address options network-address
```

Many options can be used with the pntadm command, which are documented in the pntadm(1M) man page.

[Table 14-4](#) shows some sample pntadm commands that specify options.

Removing IP Addresses From the DHCP Service

At times, you might want the DHCP service to stop managing a particular IP address or group of addresses. The method that you use to remove an address from DHCP depends on whether you want the change to be temporary or permanent.

- To temporarily prevent the use of addresses, you can mark the addresses as unusable in the Address Properties dialog box as described in [“Marking IP Addresses as Unusable by the DHCP Service”](#) on page 334.
- To permanently prevent the use of addresses by DHCP clients, delete the addresses from the DHCP network tables, as described in [“Deleting IP Addresses From the DHCP Service”](#) on page 336.

Marking IP Addresses as Unusable by the DHCP Service

You can use the pntadm -M command with the -f UNUSABLE option to mark addresses as unusable.

In DHCP Manager, you use the Address Properties dialog box, shown in [Figure 14-10](#), to mark individual addresses. You use the Modify Multiple Addresses dialog box, shown in [Figure 14-11](#), to mark multiple addresses, as described in the following procedure.

▼ How to Mark IP Addresses as Unusable (DHCP Manager)

- Steps**
1. **In DHCP Manager, select the Addresses tab.**
See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.
 2. **Select the IP address’s network.**
 3. **Select one or more IP addresses to mark as unusable.**
If you want to mark more than one address as unusable, press the Control key while you click with the mouse to select multiple addresses. You can also press the Shift key while you click to select a block of addresses.
 4. **Choose Properties from the Edit menu.**
The Address Properties dialog box or the Modify Multiple Address dialog box opens.
 5. **If you are modifying one address, select the Lease tab.**
 6. **Select Address is Unusable.**
If you are editing multiple addresses, select Mark All Addresses Unusable.
 7. **Click OK.**

▼ How to Mark IP Addresses as Unusable (pntadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.
 2. **Mark IP addresses as unusable by typing a command of the following format:**

```
# pntadm -M ip-address -f UNUSABLE network-address
```


For example, to mark address 10.64.3.3 as unusable, type:

```
pntadm -M 10.64.3.3 -f UNUSABLE 10.64.3.0
```

Deleting IP Addresses From the DHCP Service

You should delete IP addresses from the DHCP network tables if you no longer want the address to be managed by DHCP. You can use the `pntadm -D` command or DHCP Manager's Delete Address dialog box.

The following figure shows the Delete Address dialog box.

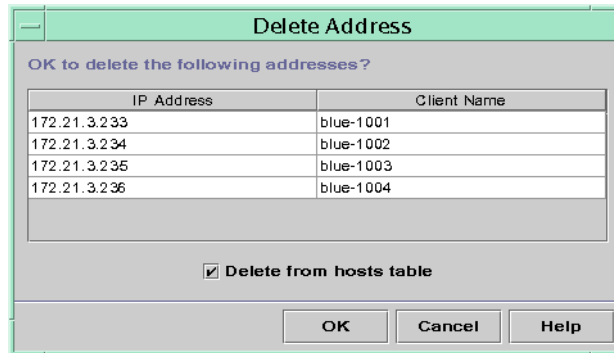


FIGURE 14-12 Delete Address Dialog Box in DHCP Manager

▼ How to Delete IP Addresses From DHCP Service (DHCP Manager)

Steps 1. In DHCP Manager, select the **Addresses** tab.

See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.

2. Select the IP address's network.

3. Select one or more IP addresses to delete.

If you want to delete more than one address, press the Control key while you click with the mouse to select multiple addresses. You can also press the Shift key while you click to select a block of addresses.

4. Choose **Delete** from the **Edit** menu.

The Delete Address dialog box lists the address that you selected so that you can confirm the deletion.

5. If you want to delete the host names from the hosts table, select **Delete From Hosts Table**.

If the host names were generated by DHCP Manager, you might want to delete the names from the hosts table.

6. Click OK.

▼ How to Delete IP Addresses From the DHCP Service (pntadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)” in *System Administration Guide: Security Services*](#).

2. **Delete IP addresses by typing a command of the following format:**

```
# pntadm -D ip-address options network-address
```

If you include the `-y` option, the host name is deleted from the name service that maintains the host name.

For example, to delete address `10.64.3.3` from network `10.64.3.0`, and delete the corresponding host name, type:

```
pntadm -D 10.64.3.3 -y 10.64.3.0
```

Assigning a Reserved IP Address to a DHCP Client

The Solaris DHCP service attempts to provide the same IP address to a client that has previously obtained an address through DHCP. However, sometimes an address has already been reassigned to another client.

Routers, NIS or NIS+ servers, DNS servers, and other hosts that are critical to the network should not be DHCP clients. Hosts that provide services to the network should not rely on the network to obtain their IP addresses. Clients such as print servers or file servers should have consistent IP addresses as well. These clients can receive their network configurations and also be assigned a consistent IP address from the DHCP server.

You can set up the DHCP server to supply the same IP address to a client each time the client requests its configuration. You reserve the IP address for the client by manually assigning the client's ID to the address that you want the client to use. You can set up the reserved address to use either a dynamic lease or a permanent lease. If the client's address uses a dynamic lease, you can easily track the use of the address. A diskless client is an example of a client that should use a reserved address with a dynamic lease. If the client's address uses a permanent lease, you cannot track address

use. Once a client obtains a permanent lease, the client does not contact the server again. The client can obtain updated configuration information only by releasing the IP address and restarting the DHCP lease negotiation.

You can use the `pnt adm -M` command or DHCP Manager's Address Properties dialog box to set up lease properties.

The following figure shows the Lease tab of the Address Properties dialog box, which is used to modify the lease.

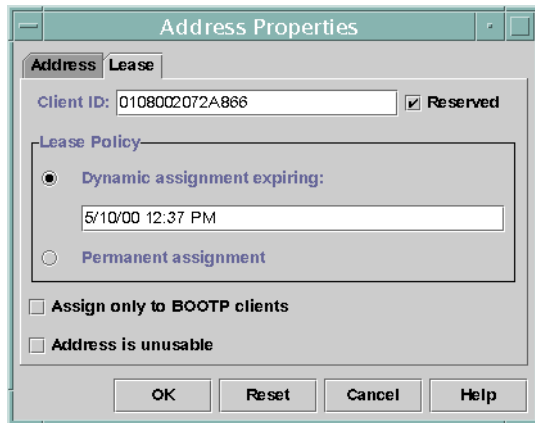


FIGURE 14-13 Address Properties Lease Tab in DHCP Manager

▼ How to Assign a Consistent IP Address to a DHCP Client (DHCP Manager)

- Steps**
1. In DHCP Manager, select the **Addresses** tab.
See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.
 2. Select the appropriate network.
 3. Double-click the IP address that you want to the client to use.
The Address Properties window opens.
 4. Select the **Lease** tab.
 5. In the **Client ID** field, type the client ID.
The client ID is derived from the client's hardware address. See the Client ID entry in Table 14-4 for more information.

6. Select the **Reserved** option to prevent the IP address from being reclaimed by the server.
7. In the **Lease Policy** area of the window, select **Dynamic or Permanent assignment**.
 Select **Dynamic** if you want the client to negotiate to renew leases, which enables you to track when the address is used. Because you selected **Reserved**, the address cannot be reclaimed even when a dynamic lease is assigned. You do not need to specify an expiration date for this lease. The DHCP server calculates the expiration date by using the lease time.
 If you select **Permanent**, you cannot track the use of the IP address unless you enable transaction logging.
8. Click **OK**.

▼ How to Assign a Consistent IP Address to a DHCP Client (pntadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
 For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).
 Roles contain authorizations and privileged commands. For more information about roles, see *“Configuring RBAC (Task Map)” in System Administration Guide: Security Services*.

2. **Set the lease flags by typing a command of the following format:**

```
# pntadm -M ip-address -i client-id -f MANUAL+BOOTP network-address
```

For example, to enable the Solaris DHCP client whose MAC address is 08:00:20:94:12:1E to always receive IP address 10.21.5.12, you would type:

```
pntadm -M 10.21.5.12 -i 0108002094121E -f MANUAL+BOOTP
10.21.0.0
```

Tip – Refer to the Client ID entry in [Table 14–4](#) for more information about how to determine client identifiers.

Working With DHCP Macros (Task Map)

DHCP macros are containers of DHCP options. The Solaris DHCP service uses macros to gather options that should be passed to clients. DHCP Manager and the `dhcpconfig` utility create a number of macros automatically when you configure the server. See [“About DHCP Macros” on page 259](#) for background information about macros. See [Chapter 13](#) for information about macros created by default.

You might find that when changes occur on your network, you need to make changes to the configuration information that is passed to clients. To change configuration information, you need to work with DHCP macros. You can view, create, modify, duplicate, and delete DHCP macros.

When you work with macros, you must know about DHCP standard options, which are described in the `dhcp_inittab(4)` man page.

The following task map lists tasks to help you view, create, modify, and delete DHCP macros.

Task	Description	For Instructions
View DHCP macros.	Display a list of all the macros that are defined on the DHCP server.	“How to View Macros Defined on a DHCP Server (DHCP Manager)” on page 341 “How to View Macros Defined on a DHCP Server (dhtadm)” on page 342
Create DHCP macros.	Create new macros to support DHCP clients.	“How to Create a DHCP Macro (DHCP Manager)” on page 347 “How to Create a DHCP Macro (dhtadm)” on page 348
Modify values that are passed in macros to DHCP clients.	Change macros by modifying existing options, adding options to macros, or removing options from macros.	“How to Change Values for Options in a DHCP Macro (DHCP Manager)” on page 343 “How to Change Values for Options in a DHCP Macro (dhtadm)” on page 344 “How to Add Options to a DHCP Macro (DHCP Manager)” on page 344 “How to Add Options to a DHCP Macro (dhtadm)” on page 345 “How to Delete Options From a DHCP Macro (DHCP Manager)” on page 345 “How to Delete Options From a DHCP Macro (dhtadm)” on page 346

Task	Description	For Instructions
Delete DHCP macros.	Remove DHCP macros that are no longer used.	“How to Delete a DHCP Macro (DHCP Manager)” on page 349 “How to Delete a DHCP Macro (dht adm)” on page 349

The following figure shows the Macros tab in the DHCP Manager window.

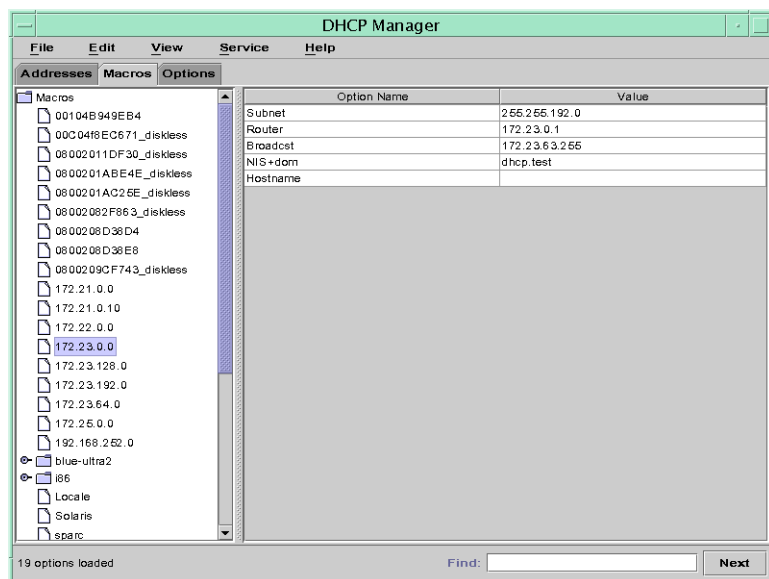


FIGURE 14–14 DHCP Manager’s Macros Tab

▼ How to View Macros Defined on a DHCP Server (DHCP Manager)

Steps 1. In DHCP Manager, select the Macros tab.

See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.

The Macros area on the left side of the window displays, in alphabetical order, all the macros defined on the DHCP server. Macros preceded by a folder icon include references to other macros, whereas macros preceded by a document icon do not reference other macros.

2. To open a macro folder, click the handle icon to the left of the folder icon.

The macros that are included in the selected macro are listed.

3. To view the content of a macro, click the macro name.

Options and their assigned values are displayed.

▼ How to View Macros Defined on a DHCP Server (dhtadm)

- Steps**
1. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

2. Display the macros by typing the following command:

```
# dhtadm -P
```

This command prints to standard output the formatted contents of the `dhcptab` table, including all macros and symbols defined on the DHCP server.

Modifying DHCP Macros

You might need to modify macros when some aspect of your network changes and one or more DHCP clients need to know about the change. For example, you might add a router or an NIS server, create a new subnet, or change the lease policy.

Before you modify a macro, determine the name of the DHCP option you want to change, add, or delete. The standard DHCP options are listed in the DHCP Manager help and in the `dhcp_inittab(4)` man page.

You can use the `dhtadm -M -m` command or DHCP Manager to modify macros. See the `dhtadm(1M)` man page for more information about `dhtadm`.

The following figure shows DHCP Manager’s Macro Properties dialog box.

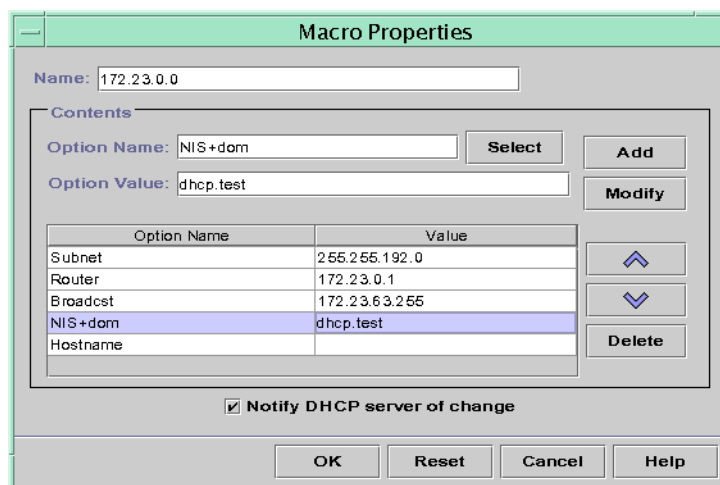


FIGURE 14–15 Macro Properties Dialog Box in DHCP Manager

▼ How to Change Values for Options in a DHCP Macro (DHCP Manager)

- Steps**
1. **In DHCP Manager, select the Macros tab.**
See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.
 2. **Select the macro that you want to change.**
 3. **Choose Properties from the Edit menu.**
The Macro Properties dialog box opens.
 4. **In the table of Options, select the option that you want to change.**
The option’s name and its value are displayed in the Option Name and Option Value fields.
 5. **In the Option Value field, select the old value and type the new value for the option.**
 6. **Click Modify.**
The new value is displayed in the options table.
 7. **Select Notify DHCP Server of Change.**
This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.

8. Click OK.

▼ How to Change Values for Options in a DHCP Macro (dhtadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)” in *System Administration Guide: Security Services*](#).

2. **Change option values by typing a command of the following format:**

```
# dhtadm -M -m macroname -e 'option=value:option=value' -g
```

For example, to change the lease time and the Universal Time Offset in the macro `bluenote`, you would type:

```
# dhtadm -M -m bluenote -e 'LeaseTim=43200:UTCOffset=28800' -g
```

▼ How to Add Options to a DHCP Macro (DHCP Manager)

- Steps**
1. **In DHCP Manager, select the Macros tab.**

See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.

2. **Select the macro that you want to change.**

3. **Choose Properties from the Edit menu.**

The Macro Properties dialog box opens.

4. **In the Option Name field, specify the name of an option by using one of the following methods:**

- **Click the Select button next to the Option Name field to select an option to add to the macro.**

The Select Option dialog box displays an alphabetized list of names of standard category options and descriptions. If you want to add an option that is not in the standard category, use the Category list to select a category.

See [“About DHCP Macros” on page 259](#) for more information about macro categories.

- **Type Include** if you want to include a reference to an existing macro in the new macro.
- 5. **Type the value for the option in the Option Value field.**
If you typed **Include** as the option name, you must specify the name of an existing macro in the Option Value field.
- 6. **Click Add.**
The option is added to the bottom of the list of options in this macro. To change the option's position in the macro, select the option and click the arrow buttons to move the option up or down in the list.
- 7. **Select Notify DHCP Server of Change.**
This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.
- 8. **Click OK.**

▼ How to Add Options to a DHCP Macro (`dhtadm`)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)” in *System Administration Guide: Security Services*](#).
 2. **Add options to a macro by typing a command of the following format:**

```
# dhtadm -M -m macroname -e 'option=value' -g
```


For example, to add the ability to negotiate leases in the macro `bluenote`, you would type the following command:

```
# dhtadm -M -m bluenote -e 'LeaseNeg=_NULL_VALUE' -g
```


Note that if an option does not require a value, you must use `_NULL_VALUE` as the value for the option.

▼ How to Delete Options From a DHCP Macro (DHCP Manager)

- Steps**
1. In DHCP Manager, select the **Macros** tab.

See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.

2. **Select the macro that you want to change.**
3. **Choose Properties from the Edit menu.**
The Macro Properties dialog box opens.
4. **Select the option that you want to remove from the macro.**
5. **Click Delete.**
The option is removed from the list of options for this macro.
6. **Select Notify DHCP Server of Change.**
This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.
7. **Click OK.**

▼ How to Delete Options From a DHCP Macro (dhtadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see “Setting Up User Access to DHCP Commands” on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Delete an option from a macro by typing a command of the following format:**

```
# dhtadm -M -m macroname -e 'option=' -g
```

For example, to remove the ability to negotiate leases in the macro `bluenote`, you would type the following command:

```
# dhtadm -M -m bluenote -e 'LeaseNeg=' -g
```

If an option is specified with no value, the option is removed from the macro.

Creating DHCP Macros

You might want to add new macros to your DHCP service to support clients with specific needs. You can use the `dhtadm -A -m` command or DHCP Manager’s Create Macro dialog box to add macros. See the `dhtadm(1M)` man page for more information about the `dhtadm` command.

The following figure shows DHCP Manager's Create Macro dialog box.

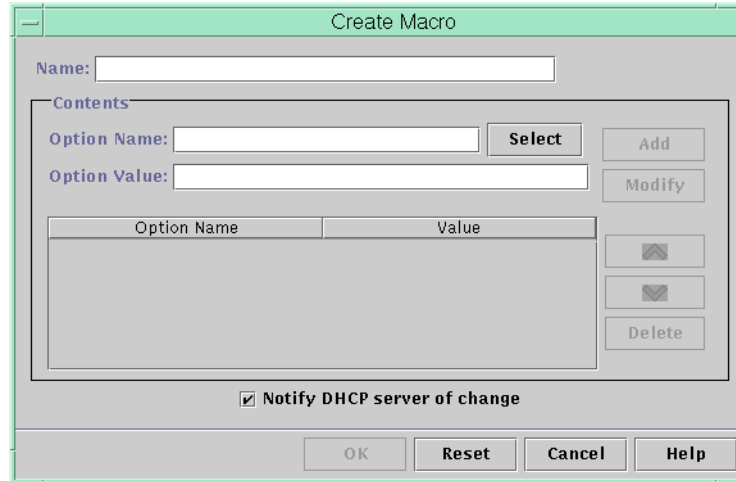


FIGURE 14-16 Create Macro Dialog Box in DHCP Manager

▼ How to Create a DHCP Macro (DHCP Manager)

- Steps**
- 1. In DHCP Manager, select the Macros tab.**
See [“How to Start and Stop DHCP Manager” on page 294](#) for information about DHCP Manager.
 - 2. Choose Create from the Edit menu.**
The Create Macro dialog box opens.
 - 3. Type a unique name for the macro.**
The name can be up to 128 alphanumeric characters. If you use a name that matches a vendor class identifier, network address, or client ID, the macro is processed automatically for appropriate clients. If you use a different name, the macro is not processed automatically. The macro must be assigned to a specific IP address or included in another macro that is processed automatically. See [“Macro Processing by the DHCP Server” on page 259](#) for more detailed information.
 - 4. Click the Select button, which is next to the Option Name field.**
The Select Option dialog box displays an alphabetized list of names of standard category options and their descriptions. If you want to add an option that is not in the standard category, use the Category list. Select the category that you want from the Category list. See [“About DHCP Options” on page 258](#) for more information about option categories.

5. **Select the option to add to the macro, and click OK.**
The Macro Properties dialog box displays the selected option in the Option Name field.
6. **Type the value for the option in the Option Value field, and click Add.**
The option is added to the bottom of the list of options in this macro. To change the option's position in the macro, select the option and click the arrow buttons to move the option up or down in the list.
7. **Repeat Step 5 and Step 6 for each option you want to add to the macro.**
8. **Select Notify DHCP Server of Change when you are finished adding options.**
This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.
9. **Click OK.**

▼ How to Create a DHCP Macro (`dhtadm`)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

2. **Create a macro by typing a command of the following format:**

```
# dhtadm -A -m macroname -d ' :option=value:option=value:option=value:' -g
```

There is no limit to the number of `option=value` pairs that can be included in the argument to `-d`. The argument must begin and end with colons, with colons between each `option=value` pair. The complete string must be enclosed in quotation marks.

For example, to create the macro `bluenote`, type the following command:

```
# dhtadm -A -m bluenote -d ' :Router=10.63.6.121\
:LeaseNeg=_NULL_VALUE:DNSserv=10.63.28.12:' -g
```

Note that if an option does not require a value, you must use `_NULL_VALUE` as the value for the option.

Deleting DHCP Macros

You might want to delete a macro from the DHCP service. For example, if you delete a network from the DHCP service, you can also delete the associated network macro.

You can use the `dhtadm -D -m` command or DHCP Manager to delete macros.

▼ How to Delete a DHCP Macro (DHCP Manager)

- Steps**
1. **In DHCP Manager, select the Macros tab.**
See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.
 2. **Select the macro to delete.**
The Delete Macro dialog box prompts you to confirm that you want to delete the specified macro.
 3. **Select Notify DHCP Server of Change.**
This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.
 4. **Click OK.**

▼ How to Delete a DHCP Macro (dhtadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.
 2. **Delete a macro by typing a command of the following format:**

```
# dhtadm -D -m macroname -g
```


For example, to delete the macro `bluenote`, you would type the following command:

```
# dhtadm -D -m bluenote -g
```

Working With DHCP Options (Task Map)

Options are keywords for network configuration parameters that the DHCP server can pass to clients. In the Solaris DHCP service, you cannot create, delete, or modify the standard DHCP options. The standard options are defined by the DHCP protocol, so the options cannot change. You can only perform tasks on options that you create for your site. For this reason, when you first set up your DHCP service, the Options tab in DHCP Manager is empty until you create options for your site.

If you create options on the DHCP server, you must also add information about the options on the DHCP client. For the Solaris DHCP client, you must edit the `/etc/dhcp/inittab` file to add entries for the new options. See the `dhcp_inittab(4)` man page for more information about this file.

If you have DHCP clients that are not Solaris clients, refer to the documentation for those clients for information about adding options or symbols. See [“About DHCP Options” on page 258](#) for more information about options in Solaris DHCP.

You can use either DHCP Manager or the `dhtadm` command to create, modify, or delete options.

Tip – Options are called *symbols* in the DHCP literature. The `dhtadm` command and its related man page also refer to options as symbols.

The following task map lists tasks that you must perform to create, modify, and delete DHCP options. The task map contains links to procedures for the tasks.

Task	Description	For Instructions
Create DHCP options.	Add new options for information not covered by a standard DHCP option.	“How to Create DHCP Options (DHCP Manager)” on page 354 “How to Create DHCP Options (dhtadm)” on page 355 “Modifying the Solaris DHCP Client’s Option Information” on page 359

Task	Description	For Instructions
Modify DHCP options.	Change properties of DHCP options you have created.	<p>“How to Modify DHCP Option Properties (DHCP Manager)” on page 356</p> <p>“How to Modify DHCP Option Properties (dhtadm)” on page 357</p>
Delete DHCP options.	Remove DHCP options that you have created.	<p>“How to Delete DHCP Options (DHCP Manager)” on page 358</p> <p>“How to Delete DHCP Options (dhtadm)” on page 359</p>

Before you create DHCP options, you should be familiar with the option properties listed in the following table.

TABLE 14-5 DHCP Option Properties

Option Property	Description
Category	<p>The <i>category</i> of an option must be one of the following:</p> <ul style="list-style-type: none"> ■ Vendor – Options specific to a client’s vendor platform, either hardware or software. ■ Site – Options specific to your site. ■ Extend – Newer options that have been added to the DHCP protocol, but not yet implemented as standard options in Solaris DHCP.
Code	<p>The <i>code</i> is a unique number that you assign to an option. The same code cannot be used for any other option within its option category. The code must be appropriate for the option category:</p> <ul style="list-style-type: none"> ■ Vendor – Code values of 1–254 for each vendor class ■ Site – Code values of 128–254 ■ Extend – Code values of 77–127

TABLE 14-5 DHCP Option Properties (Continued)

Option Property	Description
Data type	<p>The <i>data type</i> specifies what kind of data can be assigned as a value for the option. The valid data types are described in the following list.</p> <ul style="list-style-type: none">■ ASCII – Text string value.■ BOOLEAN – No value is associated with the Boolean data type. The presence of the option indicates that a condition is true, while the absence of the option indicates that a condition is false. For example, the <code>Hostname</code> option is Boolean. The presence of <code>Hostname</code> in a macro causes the DHCP server to look up the host name associated with the assigned address.■ IP – One or more IP addresses, in dotted decimal format (<i>xxx.xxx.xxx.xxx</i>).■ OCTET – Uninterpreted ASCII representation of binary data. For example, a client ID uses the octet data type. Valid characters are 0–9, A–F, and a–f. Two ASCII characters are needed to represent an 8-bit quantity.■ UNNUMBER8, UNNUMBER16, UNNUMBER32, UNNUMBER64, SNUMBER8, SNUMBER16, SNUMBER32, or SNUMBER64 – Numeric value. An initial U or S indicates whether the number is unsigned or signed. The digits at the end indicate how many bits are in the number.
Granularity	<p>The <i>granularity</i> specifies how many “instances” of the data type are needed to represent a complete option value. For example, a data type of IP and a granularity of 2 would mean that the option value must contain two IP addresses.</p>
Maximum	<p>The maximum number of values that can be specified for the option. For example, suppose the maximum is 2, the granularity is 2, and the data type is IP. In this case, the option value could contain a maximum of two pairs of IP addresses.</p>

TABLE 14-5 DHCP Option Properties (Continued)

Option Property	Description
Vendor client classes	<p>This option is available only when the option category is Vendor. Vendor client classes identify the client classes with which the Vendor option is associated. The class is an ASCII string that represents the client machine type or operating system. For example, the class string for some models of Sun workstations is <code>SUNW.Sun-Blade-100</code>. This type of option enables you to define configuration parameters that are passed to all clients of the same class, and <i>only</i> clients of that class.</p> <p>You can specify multiple client classes. Only those DHCP clients with a client class value that matches a class that you specify receive the options scoped by that class.</p> <p>The client class is determined by the vendor of the DHCP client. For DHCP clients that are not Solaris clients, refer to the vendor documentation for the DHCP client for the client class.</p> <p>For Solaris clients, the Vendor client class can be obtained by typing the <code>uname -i</code> command on the client. To specify the Vendor client class, substitute periods for any commas in the string returned by the <code>uname</code> command. For example, if the string <code>SUNW,Sun-Blade-100</code> is returned by the <code>uname -i</code> command, you should specify the Vendor client class as <code>SUNW.Sun-Blade-100</code>.</p>

Creating DHCP Options

If you need to pass client information for which there is not already an existing option in the DHCP protocol, you can create an option. See the `dhcp_inittab(4)` man page for a list of all the options that are defined in Solaris DHCP before you create your own option.

You can use the `dhtadm -A -s` command or DHCP Manager's Create Option dialog box to create new options.

The following figure shows DHCP Manager's Create Option dialog box.

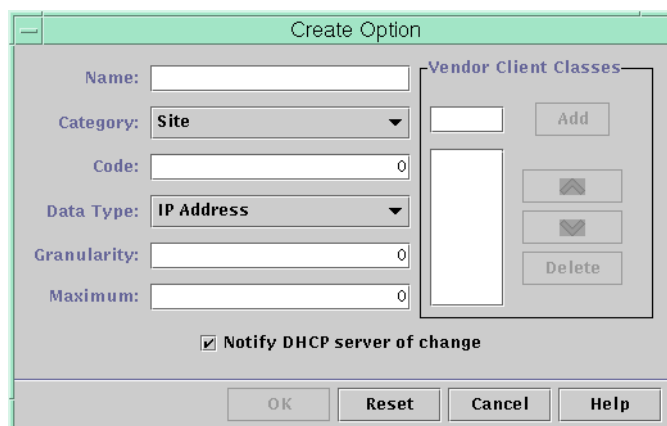


FIGURE 14-17 Create Option Dialog Box in DHCP Manager

▼ How to Create DHCP Options (DHCP Manager)

- Steps**
- 1. In DHCP Manager, select the Options tab.**
See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.
 - 2. Choose Create from the Edit menu.**
The Create Options dialog box opens.
 - 3. Type a short descriptive name for the new option.**
The name can contain up to 128 alphanumeric characters and spaces.
 - 4. Type or select values for each setting in the dialog box.**
Refer to Table 14-5 for information about each setting, or view the DHCP Manager help.
 - 5. Select Notify DHCP Server of Change if you are finished creating options.**
This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.
 - 6. Click OK.**
You can now add the option to macros, and assign a value to the option to pass to clients.

▼ How to Create DHCP Options (dhtadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see “Setting Up User Access to DHCP Commands” on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Create a DHCP option by typing a command using the following format:**

```
# dhtadm -A -s option-name -d 'category,code,data-type,granularity,maximum' -g
```

option-name Is an alphanumeric string of 128 characters or less.

category Is one of the following: Site, Extend, or Vendor=*list-of-classes*. *list-of-classes* is a space-separated list of vendor client classes to which the option applies. See Table 14-5 for information about how to determine the vendor client class.

code Is a numeric value that is appropriate to the option category, as explained in Table 14-5.

data-type Is specified by a keyword that indicates the type of data that is passed with the option, as explained in Table 14-5.

granularity Is specified as a nonnegative number, as explained in Table 14-5.

maximum Is a nonnegative number, as explained in Table 14-5.

Example 14-3 Creating a DHCP Option With dhtadm

The following command would create an option called NewOpt, which is a Site category option. The option's code is 130. The option's value can be set to a single 8-bit unsigned integer.

```
# dhtadm -A -s NewOpt -d 'Site,130,UNNUMBER8,1,1' -g
```

The following command would create an option called NewServ, which is a Vendor category option that applies to clients whose machine type is SUNW, Sun-Blade-100 or SUNW, Sun-Blade-1000. The option's code is 200. The option's value can be set to one IP address.

```
# dhtadm -A -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \ SUNW.Sun-Blade-1000,200,IP,1,1' -g
```

Modifying DHCP Options

If you have created options for your DHCP service, you can change the properties for these options. You can use the `dhtadm -M -s` command or DHCP Manager's Option Properties dialog box to modify options.

Note that you should modify the Solaris DHCP client's option information to reflect the same modification that you make to the DHCP service. See [“Modifying the Solaris DHCP Client's Option Information”](#) on page 359.

The following figure shows DHCP Manager's Option Properties dialog box.

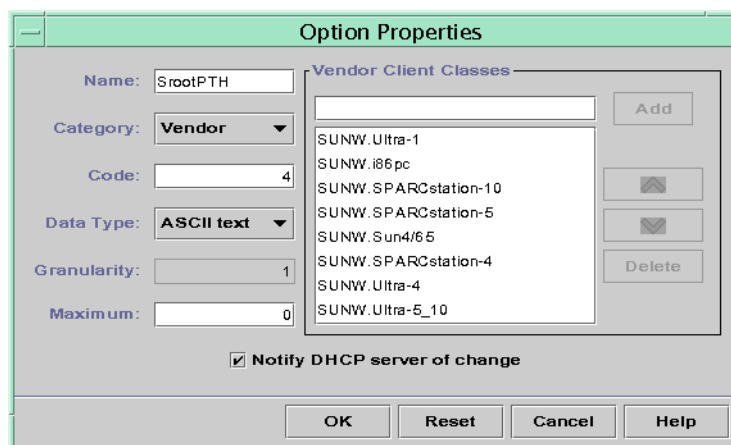


FIGURE 14-18 Option Properties Dialog Box in DHCP Manager

▼ How to Modify DHCP Option Properties (DHCP Manager)

- Steps**
1. In DHCP Manager, select the Options tab.
See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.
 2. Select the option that you want to modify.
 3. Choose Properties from the Edit menu.
The Option Properties dialog box opens.
 4. Edit the properties as needed.

See [Table 14-5](#) for information about the properties, or view the DHCP Manager help.

5. **Select Notify DHCP Server of Change when you are finished with options.**
The change is made to the `dhcptab` table. The DHCP server is signaled to reread the `dhcptab` table to put the changes into effect.
6. **Click OK.**

▼ How to Modify DHCP Option Properties (`dhtadm`)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

2. **Modify an option by typing a command using the following format:**

```
# dhtadm -M -s option-name -d 'category,code,data-type,granularity,maximum' -g
```

<i>option-name</i>	Specifies the name of the option that you want to change.
<i>category</i>	Can be <code>Site</code> , <code>Extend</code> , or <code>Vendor=list-of-classes</code> . <i>list-of-classes</i> is a space-separated list of vendor client classes to which the option applies. For example, <code>SUNW.Sun-Blade-100 SUNW.Ultra-80 SUNWi86pc</code> .
<i>code</i>	Specifies a numeric value that is appropriate to the option category, as explained in Table 14-5 .
<i>data-type</i>	Specifies a keyword that indicates the type of data that is passed with the option, as explained in Table 14-5 .
<i>granularity</i>	Is a nonnegative number, as explained in Table 14-5 .
<i>maximum</i>	Is a nonnegative number, as explained in Table 14-5 .

Note that you must specify all of the DHCP option properties with the `-d` switch, not just the properties that you want to change.

Example 14–4 Modifying a DHCP Option With `dhtadm`

The following command would modify an option called `NewOpt`. The option is a Site category option. The option's code is 135. The option's value can be set to a single 8-bit unsigned integer.

```
# dhtadm -M -s NewOpt -d 'Site,135,UNNUMBER8,1,1'
```

The following command would modify an option called `NewServ`, which is a Vendor category option. The option now applies to clients whose machine type is `SUNW, Sun-Blade-100` or `SUNW, i86pc`. The option's code is 200. The option's value can be set to one IP address.

```
# dhtadm -M -s NewServ -d 'Vendor=SUNW.Sun-Blade-100 \
SUNW.i86pc,200,IP,1,1' -g
```

Deleting DHCP Options

You cannot delete standard DHCP options. However, if you have defined options for your DHCP service, you can delete these options by using DHCP Manager or the `dhtadm` command.

▼ How to Delete DHCP Options (DHCP Manager)

Steps 1. In DHCP Manager, select the Options tab.

See [“How to Start and Stop DHCP Manager”](#) on page 294 for information about DHCP Manager.

2. Select the option that you want to delete.

3. Choose Delete from the Edit menu.

The Delete Option dialog box opens.

4. Select Notify DHCP Server of Change if you are finished deleting options.

This selection tells the DHCP server to reread the `dhcptab` table to put the change into effect immediately after you click OK.

5. Click OK.

▼ How to Delete DHCP Options (dhtadm)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.
 2. **Delete a DHCP option by typing a command using the following format:**

```
# dhtadm -D -s option-name -g
```

Modifying the Solaris DHCP Client’s Option Information

If you add a new DHCP option to your DHCP server, you must add a complementary entry to each DHCP client’s option information. If you have a DHCP client that is not a Solaris DHCP client, refer to that client’s documentation for information about adding options or symbols.

On a Solaris DHCP client, you must edit the `/etc/dhcp/inittab` file and add an entry for each option that you add to the DHCP server. If you later modify the option on the server, you must also modify the entry in the client’s `/etc/dhcp/inittab` file.

Refer to the `dhcp_inittab(4)` man page for detailed information about the syntax of the `/etc/dhcp/inittab` file.

Note – If you added DHCP options to the `dhcptags` file in a previous Solaris release, you must add the options to the `/etc/dhcp/inittab` file. See [“DHCP Option Information”](#) on page 418 for more information.

Supporting Solaris Network Installation With the DHCP Service

You can use DHCP to install the Solaris Operating System on certain client systems on your network. Only sun4u-based systems and x86 systems that meet the hardware requirements for running the Solaris OS can use this feature. For information about using DHCP to automatically configure client systems for the network as they boot, see Chapter 4, “Preconfiguring System Configuration Information (Tasks),” in *Solaris 10 Installation Guide: Network-Based Installations*.

DHCP also supports Solaris client systems that boot and install remotely from servers across a wide area network (WAN) using HTTP. This method of remote booting and installing is called the *WAN boot installation* method. Using WAN boot, you can install the Solaris OS on SPARC based systems over a large public network where the network infrastructure might be untrustworthy. You can use WAN boot with security features to protect data confidentiality and installation image integrity.

Before you can use DHCP for booting and installing client systems remotely using WAN boot, the DHCP server must be configured to supply the following information to clients:

- The proxy server’s IP address
- The location of the `wanboot-cgi` program

For details about configuring the DHCP server to provide this information, see Chapter 4, “Preconfiguring System Configuration Information (Tasks),” in *Solaris 10 Installation Guide: Network-Based Installations*. For information about booting and installing client systems with a DHCP server across a WAN, see Chapter 9, “WAN Boot (Overview),” in *Solaris 10 Installation Guide: Network-Based Installations*.

For information about supporting diskless clients, see “Supporting Remote Boot and Diskless Boot Clients (Task Map)” on page 361.

Supporting Remote Boot and Diskless Boot Clients (Task Map)

The Solaris DHCP service can support Solaris client systems that mount their operating system files remotely from another machine (the OS server). Such clients are often called *diskless clients*. Diskless clients can be thought of as persistent remote boot clients. Each time a diskless client boots, the client must obtain the name and IP address of the server that hosts the client's operating system files. The diskless client can then boot remotely from those files.

Each diskless client has its own root partition on the OS server, which is shared to the client host name. The DHCP server must always return the same IP address to a diskless client. That address must remain mapped to the same host name in the name service, such as DNS. When a diskless client receives a consistent IP address, the client uses a consistent host name, and can access its root partition on the OS server.

In addition to providing the IP address and host name, the DHCP server can supply the location of the diskless client's operating system files. However, you must create options and macros to pass the information in a DHCP message packet.

The following task map lists the tasks required to support diskless clients or any other persistent remote boot clients. The task map also provides links to procedures to help you carry out the tasks.

Task	Description	For Instructions
Set up OS services on a Solaris server.	Use the <code>smoservice</code> command to create operating system files for clients.	Chapter 7, "Managing Diskless Clients (Tasks)," in <i>System Administration Guide: Basic Administration</i> Also, see the <code>smoservice(1M)</code> man page.
Set up the DHCP service to support network boot clients.	Use DHCP Manager or the <code>dhtadm</code> command to create new Vendor options and macros, which the DHCP server can use to pass booting information to the clients. If you already created the options for network install clients, you need only to create macros for the Vendor client types of the diskless clients.	Chapter 4, "Preconfiguring System Configuration Information (Tasks)," in <i>Solaris 10 Installation Guide: Network-Based Installations</i>

Task	Description	For Instructions
Assign reserved IP addresses to the diskless clients.	Use DHCP Manager to mark address as reserved, or use the <code>pntadm</code> command to mark addresses as <code>MANUAL</code> for diskless clients.	“Assigning a Reserved IP Address to a DHCP Client” on page 337
Set up diskless clients for OS service.	Use the <code>smdiskless</code> command to add operating system support on the OS server for each client. Specify the IP addresses that you reserved for each client.	Chapter 7, “Managing Diskless Clients (Tasks),” in <i>System Administration Guide: Basic Administration</i> Also, see the <code>smdiskless(1M)</code> man page.

Setting Up DHCP Clients to Receive Information Only (Task Map)

In some networks, you might want the DHCP service to provide only configuration information to clients. Client systems that need information, not leases, can use the DHCP client to issue an `INFORM` message. The `INFORM` message asks the DHCP server to send the appropriate configuration information to the client.

You can set up the Solaris DHCP server to support clients that need information only. You need to create an empty network table that corresponds to the network that is hosting the clients. The table must exist so that the DHCP server can respond to clients from that network.

The following task map lists the tasks required to support information-only clients. The task map also includes links to procedures to help you carry out the tasks.

Task	Description	For Instructions
Create an empty network table.	Use DHCP Manager or the <code>pntadm</code> command to create a network table for the information-only clients’ network.	“Adding DHCP Networks” on page 314
Create macros to contain information that is needed by clients.	Use DHCP Manager or the <code>dhtadm</code> command to create macros to pass the required information to clients.	“Creating DHCP Macros” on page 346

Task	Description	For Instructions
Have the DHCP client issue an INFORM message.	Use the <code>ifconfig int dhcp inform</code> command to make the DHCP client issue an INFORM message.	“DHCP Client Startup” on page 374 “ifconfig Command Options Used With the DHCP Client” on page 377 ifconfig(1M)man page

Converting to a New DHCP Data Store

Solaris DHCP provides a utility to convert the DHCP configuration data from one data store to another data store. Several reasons might exist for converting to a new data store. For example, you might have more DHCP clients, requiring higher performance or higher capacity from the DHCP service. You also might want to share the DHCP server duties among multiple servers. See [“Choosing the DHCP Data Store” on page 269](#) for a comparison of the relative benefits and drawbacks of each type of data store.

Note – If you upgraded from a Solaris release that is older than the Solaris 8 7/01 release, you should read this note.

When you run any Solaris DHCP tool after Solaris installation, you are prompted to convert to the new data store. The conversion is required because the format of the data stored in both files and NIS+ changed in the Solaris 8 7/01 release. If you do not convert to the new data store, the DHCP server continues to read the old data tables. However, the server can only extend leases for existing clients. You cannot register new DHCP clients or use DHCP management tools with the old data tables.

The conversion utility is also useful for sites that are converting from a Sun provided data store to a third-party data store. The conversion utility looks up entries in the existing data store and adds new entries that contain the same data to the new data store. Data store access is implemented in separate modules for each data store. This modular approach enables the conversion utility to convert DHCP data from any data store format to any other data store format. Each data store must have a module that the DHCP service can use. See *Solaris DHCP Service Developer's Guide* for more information about how to write a module to support a third-party data store.

The data store conversion can be accomplished with DHCP Manager through the Data Store Conversion wizard, or with the `dhcpconfig -C` command.

The initial dialog box of the Data Store Conversion wizard is shown in the following figure.

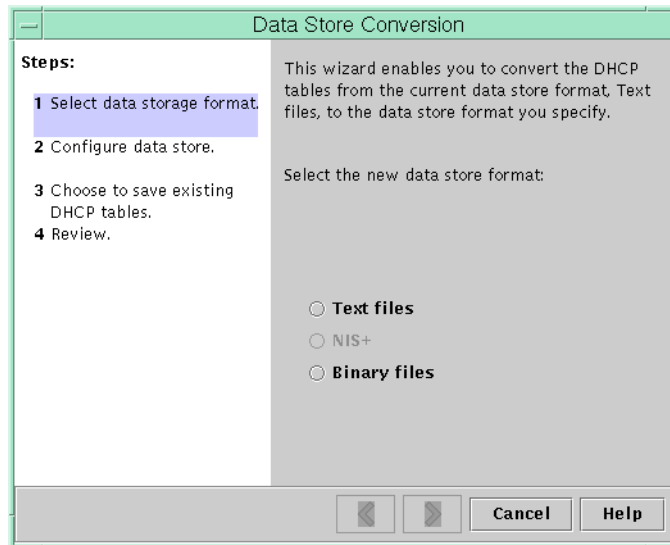


FIGURE 14–19 Data Store Conversion Wizard Dialog Box in DHCP Manager

Before the conversion begins, you must specify whether to save the old data store's tables (`dhcptab` and network tables). The conversion utility then stops the DHCP server, converts the data store, and restarts the server when the conversion has completed successfully. If you did not specify to save the old tables, the utility deletes the tables after determining the conversion is successful. The process of converting can be time-consuming. The conversion runs in the background with a meter to inform you of its progress.

▼ How to Convert the DHCP Data Store (DHCP Manager)

- Steps**
- 1. In DHCP Manager, choose Convert Data Store from the Service menu.**
See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.
The Data Store Conversion wizard opens.
 - 2. Answer the wizard's prompts.**
If you have trouble providing the requested information, click Help to view detailed information about each dialog box.
 - 3. Review your selections, and then click Finish to convert the data store.**
The DHCP server restarts when the conversion is complete. The server immediately uses the new data store.

▼ How to Convert the DHCP Data Store (`dhcpconfig -C`)

- Steps**
1. **Become superuser or assume a role or user name that is assigned to the DHCP Management profile.**
For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands” on page 295](#).
Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)” in *System Administration Guide: Security Services*](#).

2. **Convert the data store by typing a command of the following format:**

```
# /usr/sbin/dhcpconfig -C -r resource -p path
```

resource is the new data store type, such as `SUNWbinfiles`

path is the path to the data, such as `/var/dhcp`

Note that if you want to keep the original data in the old data store after the conversion, specify the `-k` option. For example, to convert your data store to `SUNWbinfiles` and save the old data store, you would type:

```
# /usr/sbin/dhcpconfig -C -r SUNWbinfiles -p /var/dhcp -k
```

See the `dhcpconfig(1M)` man page for more information about the `dhcpconfig` utility.

Moving Configuration Data Between DHCP Servers (Task Map)

DHCP Manager and the `dhcpconfig` utility enable you to move some or all the DHCP configuration data from one Solaris DHCP server to another server. You can move entire networks and all the IP addresses, macros, and options associated with the networks. Alternatively, you can select specific IP addresses, macros, and options to move. You can also copy macros and options without removing the macros and options from the first server.

You might want to move data if you are going to do any of the following tasks:

- Add a server to share DHCP duties.
- Replace the DHCP server's system.
- Change the path for the data store, while still using the same data store.

The following task map identifies the procedures that you must perform when you move DHCP configuration data.

Task	Description	For Instructions
1. Export the data from the first server.	Select the data that you want to move to another server, and create a file of exported data.	“How to Export Data From a DHCP Server (DHCP Manager)” on page 367 “How to Export Data From a DHCP Server (dhcpconfig -x)” on page 368
2. Import the data to the second server.	Copy exported data to another DHCP server’s data store.	“How to Import Data on a DHCP Server (DHCP Manager)” on page 369 “How to Import Data on a DHCP Server (dhcpconfig -I)” on page 369
3. Modify the imported data for the new server environment.	Change server-specific configuration data to match the new server’s information.	“How to Modify Imported DHCP Data (DHCP Manager)” on page 370 “How to Modify Imported DHCP Data (pntadm, dhtadm)” on page 370

In DHCP Manager, you use the Export Data wizard and the Import Data wizard to move the data from one server to the other server. You then modify macros in the Macros tab. The following figures show the initial dialog boxes for the wizards.

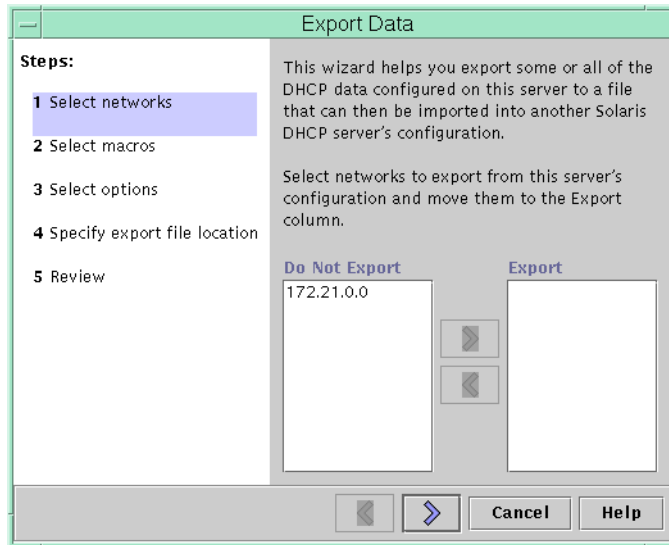


FIGURE 14–20 Export Data Wizard Dialog Box in DHCP Manager

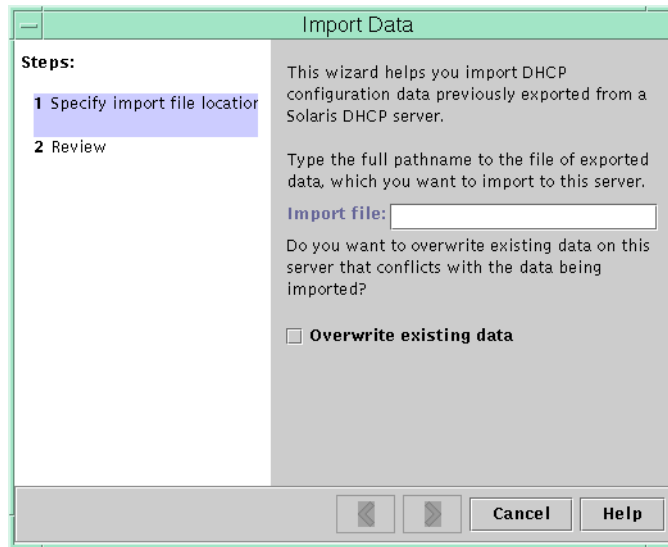


FIGURE 14-21 Import Data Wizard Dialog Box in DHCP Manager

▼ How to Export Data From a DHCP Server (DHCP Manager)

- Steps**
1. **Start DHCP Manager on the server from which you want to move or copy data.**
See “[How to Start and Stop DHCP Manager](#)” on page 294 for information about DHCP Manager.
 2. **Choose Export Data from the Service menu.**
The Export Data wizard opens as shown in [Figure 14-20](#).
 3. **Answer the wizard’s prompts.**
If you have difficulty, click Help for detailed information about the prompts.
 4. **Move the export file to a file system that is accessible to the DHCP server that must import the data.**

See Also Import the data as described in “[How to Import Data on a DHCP Server \(DHCP Manager\)](#)” on page 369.

▼ How to Export Data From a DHCP Server (`dhcpconfig -X`)

- Steps**
1. Log in to the server from which you want to move or copy data.
 2. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.
For more information about the DHCP Management profile, see “Setting Up User Access to DHCP Commands” on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

3. Export the data.

You can export all of the DHCP data, or specific parts of the data.

- To export specific addresses, macros, and options, type a command that uses the following format:

```
# dhcpconfig -X filename -a network-addresses -m macros -o options
```

filename is the full path name that you want to use to store the compressed exported data. You specify particular network addresses, DHCP macros, and DHCP options in comma-separated lists. The following example shows how to export specific networks, macros, and options.

```
# dhcpconfig -X /var/dhcp/0dhcp1065_data \  
-a 10.63.0.0,10.62.0.0 \  
-m 10.63.0.0,10.62.0.0,SUNW.Sun-Blade-100 -o Sterm
```

- To export all DHCP data, type a command that uses the ALL keyword.

```
# dhcpconfig -X filename -a ALL -m ALL -o ALL
```

filename is the full path name that you want to use to store the compressed exported data. The keyword ALL can be used with the command options to export all the network addresses, macros, or options. The following example shows how to use the ALL keyword.

```
# dhcpconfig -X /var/dhcp/dhcp1065_data -a ALL -m ALL -o ALL
```

Tip – You can omit the export of a particular kind of data by not specifying the `dhcpconfig` command option for that type of data. For example, if you do not specify the `-m` option, no DHCP macros are exported.

See the `dhcpconfig(1M)` man page for more information about the `dhcpconfig` command.

4. Move the export file to a location that is accessible to the server that must import the data.

See Also Import the data as described in “How to Import Data on a DHCP Server (`dhcpconfig -I`)” on page 369.

▼ How to Import Data on a DHCP Server (DHCP Manager)

- Steps**
1. Start DHCP Manager on the server to which you want to move data that you previously exported from a DHCP server.
See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.
 2. Choose Import Data from the Service menu.
The Import Data wizard opens, as shown in Figure 14–21.
 3. Answer the wizard’s prompts.
If you have difficulty, click Help for detailed information about the prompts.
 4. Modify the imported data, if necessary.
See “How to Modify Imported DHCP Data (DHCP Manager)” on page 370

▼ How to Import Data on a DHCP Server (`dhcpconfig -I`)

- Steps**
1. Log in to the server to which you want to import the data.
 2. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.
For more information about the DHCP Management profile, see “Setting Up User Access to DHCP Commands” on page 295.
Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.
 3. Import the data by typing a command of the following format:

```
# dhcpconfig -I filename
```

filename is the name of the file that contains the exported data.
 4. Modify the imported data, if necessary.

See “How to Modify Imported DHCP Data (pntadm, dhtadm)” on page 370.

▼ How to Modify Imported DHCP Data (DHCP Manager)

- Steps**
- 1. Start DHCP Manager on the server to which you imported data.**
See “How to Start and Stop DHCP Manager” on page 294 for information about DHCP Manager.
 - 2. Examine imported data for network-specific information that needs modification.**
For example, if you moved networks, you must open the Addresses tab and change the owning server of addresses in the imported networks. You might also need to open the Macros tab to specify the correct domain names for NIS, NIS+ or DNS in some macros.
 - 3. Open the Addresses, tab and select a network that you imported.**
 - 4. To select all the addresses, click the first address, press and hold the Shift key, and click the last address.**
 - 5. From the Edit menu, choose Properties.**
The Modify Multiple Addresses dialog box opens.
 - 6. At the Managing Server prompt, select the new server’s name.**
 - 7. At the Configuration Macro prompt, select the macro that should be used for all clients on this network, and then click OK.**
 - 8. Open the Macros tab.**
 - 9. Use the Find button to locate the options that are likely to need modified values.**
The Find button is located at the bottom of the window.
DNSdmain, DNSserv, NISServs, NIS+serv, and NISdmain are examples of options that might need modification on the new server.
 - 10. Change the options in the appropriate macros.**
See “How to Modify DHCP Option Properties (DHCP Manager)” on page 356 for the procedure for changing options.

▼ How to Modify Imported DHCP Data (pntadm, dhtadm)

- Steps**
- 1. Log in to the server to which you imported data.**

2. Become superuser or assume a role or user name that is assigned to the DHCP Management profile.

For more information about the DHCP Management profile, see [“Setting Up User Access to DHCP Commands”](#) on page 295.

Roles contain authorizations and privileged commands. For more information about roles, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

3. Examine the network tables for data that needs to be modified.

If you moved networks, use the `pntadm -P network-address` command to print out the network tables for the networks you moved.

4. Modify IP address information by using the `pntadm` command.

You might need to change the owning server and the configuration macro for imported addresses. For example, to change the owning server (10.60.3.4) and macro (dhcprsv-1060) for address 10.63.0.2, you would use the following command:

```
pntadm -M 10.63.0.2 -s 10.60.3.4 -m dhcprsv-1060 10.60.0.0
```

If you have a large number of addresses, you should create a script file that contains commands to modify each address. Execute the script with the `pntadm -B` command, which runs `pntadm` in batch mode. See the `pntadm(1M)` man page.

5. Examine the `dhcptab` macros for options with values that need modification.

Use the `dhtadm -P` command to print the entire `dhcptab` table to your screen. Use `grep` or some other tool to search for options or values that you might want to change.

6. Modify options in macros, if necessary, by using the `dhtadm -M` command.

For example, you might need to modify some macros to specify the correct domain names and servers for NIS, NIS+ or DNS. For example, the following command changes the values of `DNSdmain` and `DNSserv` in the macro `mymacro`:

```
dhtadm -M -m mymacro -e 'DNSserv=dnsrv2:DNSdmain=example.net' -g
```


Configuring and Administering the DHCP Client

This chapter discusses the Solaris DHCP client. The chapter explains how the client works, and how you can affect the client's behavior.

This chapter contains the following information:

- [“About the Solaris DHCP Client” on page 373](#)
- [“Enabling and Disabling a Solaris DHCP Client” on page 375](#)
- [“DHCP Client Administration” on page 377](#)
- [“DHCP Client Systems With Multiple Network Interfaces” on page 379](#)
- [“DHCP Client Host Names” on page 380](#)
- [“DHCP Client Systems and Name Services” on page 381](#)
- [“DHCP Client Event Scripts” on page 386](#)

About the Solaris DHCP Client

The Solaris DHCP client is the `dhcpagent` daemon, which is part of the Solaris Operating System (Solaris OS). When you install the Solaris OS, you are prompted to use DHCP to configure network interfaces. If you specify Yes, the DHCP client software is enabled on your system during Solaris installation. You do not need to do anything else with the Solaris client to use DHCP. The DHCP server's configuration determines what information is given to DHCP client systems that use the DHCP service.

If a client system is already running the Solaris OS, but not using DHCP, you can reconfigure the client system to use DHCP. You can also reconfigure a DHCP client system so that it stops using DHCP and uses static network information that you provide. See [“Enabling and Disabling a Solaris DHCP Client” on page 375](#) for more information.

DHCP Client Startup

The `dhcpcd` daemon obtains configuration information that is needed by other processes involved in booting the system. For this reason, the system startup scripts start `dhcpcd` early in the boot process and wait until the network configuration information from the DHCP server arrives.

The presence of the file `/etc/dhcp.interface` (for example, `/etc/dhcp.ce0` on a Sun Fire™ 880 system) indicates to the startup scripts that DHCP is to be used on the specified interface. Upon finding a `dhcp.interface` file, the startup scripts start `dhcpcd`.

After startup, `dhcpcd` waits until it receives instructions to configure a network interface. The startup scripts issue the `ifconfig interface dhcp start` command, which instructs `dhcpcd` to start DHCP as described in [“How DHCP Works” on page 249](#). If commands are contained within the `dhcp.interface` file, they are appended to the `dhcp start` option of `ifconfig`. See the `ifconfig(1M)` man page for more information about options used with the `ifconfig interface dhcp` command.

How the DHCP Client Manages Network Configuration Information

After the information packet is obtained from a DHCP server, `dhcpcd` configures the network interface and brings up the interface. The daemon controls the interface for the duration of the lease time for the IP address, and maintains the configuration data in an internal table. The system startup scripts use the `dhcpcinfo` command to extract configuration option values from the internal table. The values are used to configure the system and enable it to communicate on the network.

The `dhcpcd` daemon waits passively until a period of time elapses, usually half the lease time. The daemon then requests an extension of the lease from a DHCP server. If `dhcpcd` finds that the interface is down or that the IP address has changed, the daemon does not control the interface until instructed by the `ifconfig` command to do so. If `dhcpcd` finds that the interface is up and the IP address hasn't changed, the daemon sends a request to the server for a lease renewal. If the lease cannot be renewed, `dhcpcd` takes down the interface at the end of the lease time.

Each time `dhcpcd` performs an action related to the lease, the daemon looks for an executable file called `/etc/dhcp/eventhook`. If an executable file with this name is found, `dhcpcd` invokes the executable. See [“DHCP Client Event Scripts” on page 386](#) for more information about using the event executable.

DHCP Client Shutdown

When the DHCP client system shuts down normally, `dhcpagent` writes the current configuration information to the file `/etc/dhcp/interface.dhc`. The lease is dropped rather than released, so the DHCP server does not know that the IP address is not in active use.

If the lease is still valid when the system reboots, `dhcpagent` sends an abbreviated request to use the same IP address and network configuration information. If the DHCP server permits this request, `dhcpagent` can use the information that it wrote to disk when the system shut down. If the server does not permit the client to use the information, `dhcpagent` initiates the DHCP protocol sequence described in [“How DHCP Works” on page 249](#). As a result, the client obtains new network configuration information.

Enabling and Disabling a Solaris DHCP Client

To enable the DHCP client on a system that is already running the Solaris OS and is not using DHCP, you must first unconfigure the system. When the system boots, you must issue some commands to set up the system and enable the DHCP client.

If your DHCP client is not a Solaris DHCP client, consult the client documentation for instructions.

Note – Routers, NIS or NIS+ servers, DNS servers, and other hosts that are critical to the network should *not* be DHCP clients. Hosts that provide services to the network should not rely on the network to obtain their IP addresses. Hosts that are print servers or file servers should have consistent IP addresses as well. However, print servers and file servers can become DHCP clients to receive their network configurations through DHCP. You can configure the DHCP server to provide consistent IP addresses to such DHCP clients, as described in [“Assigning a Reserved IP Address to a DHCP Client” on page 337](#).

▼ How to Enable the Solaris DHCP Client

This procedure is necessary only if DHCP was not enabled during Solaris installation.

- Steps**
1. **Become superuser on the client system.**

2. If this system uses preconfiguration instead of interactive configuration, edit the `sysidcfg` file. Add the `dhcp` subkey to the `network_interface` keyword in the `sysidcfg` file.

For example, `network_interface=hme0 {dhcp}`. See the `sysidcfg(4)` man page for more information.

3. Unconfigure and shut down the system.

```
# sys-unconfig
```

See the `sys-unconfig(1M)` man page for more information about the configuration information that is removed by this command.

4. Reboot the system after shutdown is complete.

If the system uses preconfiguration, the `dhcp` subkey in the `sysidcfg` file configures the system to use the DHCP client as the system boots.

If the system does not use preconfiguration, you are prompted for system configuration information by `sysidtool` programs when the system reboots. See the `sysidtool(1M)` man page for more information.

5. When prompted to use DHCP to configure network interfaces, specify Yes.

▼ How to Disable a Solaris DHCP Client

- Steps** 1. Become superuser on the client system.

2. If you used a `sysidcfg` file to preconfigure the system, remove the `dhcp` subkey from the `network_interface` keyword.

3. Unconfigure and shut down the system.

```
# sys-unconfig
```

See the `sys-unconfig(1M)` man page for more information about the configuration information that is removed by this command.

4. Reboot the system after shutdown is complete.

If the system uses preconfiguration, you are not prompted for configuration information, and the DHCP client is not configured.

If the system does not use preconfiguration, you are prompted for system configuration information by `sysidtool` programs when the system reboots. See the `sysidtool(1M)` man page for more information.

5. When prompted to use DHCP to configure network interfaces, specify No.

DHCP Client Administration

The Solaris DHCP client software does not require administration under normal system operation. The `dhcpcagent` daemon automatically starts when the system boots, renegotiates leases, and stops when the system shuts down. You cannot manually start and stop the `dhcpcagent` daemon directly. However, as superuser on the client system, you can use the `ifconfig` command to affect `dhcpcagent`'s management of the network interface, if necessary.

`ifconfig` Command Options Used With the DHCP Client

The `ifconfig` command enables you to do the following:

- **Start the DHCP client** – The command `ifconfig interface dhcp start` initiates the interaction between `dhcpcagent` and the DHCP server to obtain an IP address and a new set of configuration options. This command is useful when you change information that you want a client to use immediately, such as when you add IP addresses or change the subnet mask.
- **Request network configuration information only** – The command `ifconfig interface dhcp inform` causes `dhcpcagent` to issue a request for network configuration parameters, with the exception of the IP address. This command is useful when the network interface has a valid IP address, but the client system needs updated network options. For example, this command is useful if you do not use DHCP to manage IP addresses, but you do use it to configure hosts on the network.
- **Request a lease extension** – The command `ifconfig interface dhcp extend` causes `dhcpcagent` to issue a request to renew the lease. The client does automatically request to renew leases. However, you might want to use this command if you change the lease time and want clients to use the new lease time immediately, rather than waiting for the next attempt at lease renewal.
- **Release the IP address** – The command `ifconfig interface dhcp release` causes `dhcpcagent` to relinquish the IP address used by the network interface. Release of the IP address happens automatically when the lease expires. You might want to issue this command if the lease time is long and you need to take down the network interface for an extended period of time. You should use this command when you remove the system from the network.
- **Drop the IP address** – The command `ifconfig interface dhcp drop` causes `dhcpcagent` to take down the network interface without informing the DHCP server. This command enables the client to use the same IP address when it reboots.
- **Ping the network interface** – The command `ifconfig interface dhcp ping` lets you determine if the interface is under the control of DHCP.

- **View the DHCP configuration status of the network interface** – The command `ifconfig interface dhcp status` displays the current state of the DHCP client. The display indicates the following items:
 - If an IP address has been bound to the client
 - The number of requests sent, received, and declined
 - If this interface is the primary interface
 - Times when the lease was obtained, when it expires, and when renewal attempts are scheduled to begin

For example:

```
# ifconfig hme0 dhcp status
Interface State      Sent  Recv  Declined  Flags
hme0      BOUND      1     1     0         [PRIMARY]
(Began,Expires,Renew)=(08/16/2005 15:27, 08/18/2005 13:31, 08/17/2005 15:24)
```

Setting DHCP Client Configuration Parameters

The `/etc/default/dhcpagent` file on the client system contains tunable parameters for the `dhcpagent`. You can use a text editor to change several parameters that affect client operation. The `/etc/default/dhcpagent` file is well documented, so for more information, you should refer to the file as well as to the `dhcpagent(1M)` man page.

The `/etc/dhcp.interface` file is another location in which parameters affecting the DHCP client are set. Parameters set in this file are used by system startup scripts with the `ifconfig` command.

By default, the DHCP client is configured as follows:

- The client system uses DHCP on one physical network interface.
If you want to use DHCP on more than one physical network interface, see [“DHCP Client Systems With Multiple Network Interfaces” on page 379](#).
- The client system does not require a particular host name.
If you want a client to request a specific host name, see [“DHCP Client Host Names” on page 380](#).
- The client is not automatically configured as a name service client if the DHCP client was configured after the Solaris installation.
See [“DHCP Client Systems and Name Services” on page 381](#) for information about using name services with DHCP clients.
- The client requests only the subnet mask, router IP address, client host name, and encapsulated vendor options.
The DHCP client’s parameter file can be set up to request more options in the `PARAM_REQUEST_LIST` keyword in the `/etc/default/dhcpagent` file. The DHCP server can be configured to provide options that were not specifically

requested. See [“About DHCP Macros” on page 259](#) and [“Working With DHCP Macros \(Task Map\)” on page 340](#) for information about using DHCP server macros to send information to clients.

DHCP Client Systems With Multiple Network Interfaces

The DHCP client can simultaneously manage several different interfaces on one system. The interfaces can be physical interfaces or logical interfaces. Each interface has its own IP address and lease time. If more than one network interface is configured for DHCP, the client issues separate requests to configure them. The client maintains a separate set of network configuration parameters for each interface. Although the parameters are stored separately, some of the parameters are global in nature. The global parameters apply to the system as a whole, rather than to a particular network interface.

The host name, NIS domain name, and time zone are global parameters and should have the same values for each interface. However, these values may differ due to errors in the information specified by the DHCP administrator. To ensure that there is only one answer to a query for a global parameter, only the parameters for the primary network interface are requested. You can insert the word `primary` in the `/etc/dhcp.interface` file for the interface that you want to be treated as the primary interface. If the `primary` keyword is not used, the first interface in alphabetical order is considered to be the primary interface.

The DHCP client manages leases for logical interfaces and physical interfaces identically, except for the following limitations on logical interfaces:

- The DHCP client does not manage the default routes that are associated with logical interfaces.

The Solaris kernel associates routes with physical interfaces, not logical interfaces. When a physical interface's IP address is established, the necessary default routes should be placed in the routing table. If DHCP is used subsequently to configure a logical interface associated with that physical interface, the necessary routes should already be in place. The logical interface uses the same routes.

When a lease expires on a physical interface, the DHCP client removes the default routes that are associated with the interface. When a lease expires on a logical interface, the DHCP client does not remove the default routes associated with the logical interface. The associated physical interface and possibly other logical interfaces might need to use the same routes.

If you need to add or remove default routes that are associated with a DHCP-controlled interface, you can use the DHCP client event script mechanism. See [“DHCP Client Event Scripts” on page 386](#).

- The DHCP client does not automatically generate client identifiers for logical interfaces.

The client identifier is used to uniquely identify a DHCP client so that it can receive configuration information that is specifically targeted to that client. For physical interfaces, the DHCP client identifier is derived from the media access control (MAC) address of the system's network interface hardware. However, no Internet standard exists for the format of DHCP client identifiers for physical interfaces that have multiple leases. You must create your own client identifier for any logical interface that you want to be configured through DHCP. The client identifier must be specified in the `/etc/default/dhclient` file with the `interface.CLIENT_ID` keyword. For example, to specify the client identifier `orangutan-ce0-1` for the logical interface `ce0:1`, you would use the following entry:

```
ce0:1.CLIENT_ID=orangutan-ce0-1
```

See the `/etc/default/dhclient` file and the `dhclient(1M)` man page for more information about the parameters you can set in the file.

If you do not configure a client identifier, `ifconfig` fails when it tries to configure the logical interface to use DHCP. The error message is:

```
ifconfig: ce0:1: interface does not have a configured DHCP client id
```

DHCP Client Host Names

By default, the Solaris DHCP client does not supply its own host name, because the client expects the DHCP server to supply the host name. The Solaris DHCP server is configured to supply host names to DHCP clients by default. When you use the Solaris DHCP client and server together, these defaults work well. However, when you use the Solaris DHCP client with some third-party DHCP servers, the client might not receive a host name from the server. If the Solaris DHCP client does not receive a host name through DHCP, the client system looks at the `/etc/nodename` file for a name to use as the host name. If the file is empty, the host name is set to `unknown`.

If the DHCP server supplies a name in the DHCP `hostname` option, the client uses that host name, even if a different value is placed in the `/etc/nodename` file. If you want the client to use a specific host name, you can enable the client to request that name. See the following procedure.

▼ How to Enable a Solaris Client to Request a Specific Host Name

- Steps**
1. On the client system, edit the `/etc/default/dhclient` file as superuser.

2. Find the `REQUEST_HOSTNAME` keyword in the `/etc/default/dhcpagent` file and modify the keyword as follows:

```
REQUEST_HOSTNAME=yes
```

If a comment sign (#) is in front of `REQUEST_HOSTNAME`, remove the #. If the `REQUEST_HOSTNAME` keyword is not present, insert the keyword.

3. Edit the `/etc/hostname.interface` file on the client system to add the following line:

```
inet hostname
```

`hostname` is the name that you want the client to use.

4. Type the following commands to have the client perform a full DHCP negotiation upon rebooting:

```
# pkill dhcpagent
# rm /etc/dhcp/interface.dhc
# reboot
```

The DHCP data that is cached on the client is removed. The client restarts the protocol to request new configuration information, including a new host name. The DHCP server first makes sure that the host name is not in use by another system on the network. The server then assigns the host name to the client. If configured to do so, the DHCP server can update name services with the client's host name.

If you want to change the host name later, repeat [Step 3](#) and [Step 4](#).

DHCP Client Systems and Name Services

Solaris systems support the following name services: DNS, NIS, NIS+, and a local file store (`/etc/inet/hosts`). Each name service requires some configuration before it is usable. The name service switch configuration file (see `nsswitch.conf(4)`) must also be set up appropriately to indicate the name services to be used.

Before a DHCP client system can use a name service, you must configure the system as a client of the name service.

The following table summarizes issues that are related to each name service and DHCP. The table includes links to documentation that can help you set up clients for each name service.

TABLE 15-1 Name Service Client Setup Information for DHCP Client Systems

Name Service	Client Setup Information
NIS	<p>If you are using Solaris DHCP to send Solaris network install information to a client system, you can use a configuration macro that contains the <code>NISservs</code> and <code>NISdomain</code> options. These options pass the IP addresses of NIS servers and the NIS domain name to the client. The client then automatically becomes an NIS client.</p> <p>If a DHCP client system is already running the Solaris OS, the NIS client is not automatically configured on that system when the DHCP server sends NIS information to the client.</p> <p>If the DHCP server is configured to send NIS information to the DHCP client system, you can see the values given to the client if you use the <code>dhcpinfo</code> command on the client as follows:</p> <pre data-bbox="623 768 948 835"># /sbin/dhchpinfo NISdomain # /sbin/dhchpinfo NISServs</pre> <p>Use the values returned for the NIS domain name and NIS servers when you set up the system as an NIS client.</p> <p>You set up an NIS client for a Solaris DHCP client system in the standard way, as documented in Chapter 5, "Setting Up and Configuring NIS Service," in <i>System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)</i>.</p> <p>Tip – You can write a script that uses <code>dhcpinfo</code> and <code>ypinit</code> to automate NIS client configuration on DHCP client systems.</p>
NIS+	<p>If the DHCP client system receives a nonreserved IP address, the address might not always be the same. You must set up the NIS+ client for a DHCP client system in a nonstandard way, which is documented in "Setting Up DHCP Clients as NIS+ Clients" on page 383. This procedure is necessary because NIS+ uses security measures to authenticate requests for service. The security measures depend upon the IP address.</p> <p>If the DHCP client system has been manually assigned an IP address, the client's address is always the same. You can set up the NIS+ client in the standard way, which is documented in "Setting Up NIS+ Client Machines" in <i>System Administration Guide: Naming and Directory Services (NIS+)</i>.</p>
<code>/etc/inet/hosts</code>	<p>You must set up the <code>/etc/inet/hosts</code> file for a DHCP client system that is to use <code>/etc/inet/hosts</code> for its name service.</p> <p>The DHCP client system's host name is added to its own <code>/etc/inet/hosts</code> file by the DHCP tools. However, you must manually add the host name to the <code>/etc/inet/hosts</code> files of other systems in the network. If the DHCP server system uses <code>/etc/inet/hosts</code> for name resolution, you must also manually add the client's host name on the system.</p>

TABLE 15-1 Name Service Client Setup Information for DHCP Client Systems (Continued)

Name Service	Client Setup Information
DNS	If the DHCP client system receives the DNS domain name through DHCP, the client system's <code>/etc/resolv.conf</code> file is configured automatically. The <code>/etc/nsswitch.conf</code> file is also automatically updated to append <code>dns</code> to the <code>hosts</code> line after any other name services in the search order. See <i>System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)</i> for more information about DNS.

Setting Up DHCP Clients as NIS+ Clients

You can use the NIS+ name service on Solaris systems that are DHCP clients. However, to do so requires you to partially circumvent one of the security-enhancing features of NIS+, the creation of Data Encryption Standard (DES) credentials. When you set up an NIS+ client that is *not* using DHCP, you add unique DES credentials for the client to the NIS+ server. There are several ways to create credentials, such as using the `nisclient` script or the `nisaddcred` command.

For DHCP clients, you *cannot* use these methods. NIS+ credential generation requires a client to have a static host name to create and store the credentials. If you want to use NIS+ and DHCP, you must create identical credentials to be used for all the host names of DHCP clients. In this way, no matter what IP address and associated host name that a DHCP client receives, the client can use the same DES credentials.



Caution – Before performing the following procedure, be aware that NIS+ was designed for increased security. This procedure weakens that security by allowing random DHCP clients to receive NIS+ credentials.

The following procedure shows you how to create identical credentials for all DHCP host names. This procedure is valid only if you know the host names that DHCP clients use. For example, when the DHCP server generates the host names, you know the possible host names that a client can receive.

▼ How to Set Up Solaris DHCP Clients as NIS+ Clients

A DHCP client system that is to be an NIS+ client must use credentials that belong to another NIS+ client system in the NIS+ domain. This procedure only produces credentials for the system, which apply only to the superuser logged in to the system. Other users who log in to the DHCP client system must have their own unique credentials in the NIS+ server. These credentials are created according to a procedure in the *System Administration Guide: Naming and Directory Services (NIS+)*.

- Steps** 1. **Create the credentials for a client by typing the following command on the NIS+ server:**

```
# nisgrep nisplus-client-name cred.org_dir > /tmp/file
```

This command writes the `cred.org_dir` table entry for the NIS+ client to a temporary file.

2. **Use the `cat` command to view the contents of the temporary file.**

Or, use a text editor.

3. **Copy the credentials to use for DHCP clients.**

You must copy the public key and private key, which are long strings of numbers and letters separated by colons. The credentials are to be pasted into the command issued in the next step.

4. **Add credentials for a DHCP client by typing the following command:**

```
# nistbladm -a cname=" dhcp-client-name@nisplus-domain" auth_type=DES \  
auth_name="unix.dhcp-client-name@nisplus-domain" \  
public_data=copied-public-key \  
private_data=copied-private-key
```

For the *copied-public-key*, paste the public key information that you copied from the temporary file. For the *copied-private-key*, paste the private key information that you copied from the temporary file.

5. **Remote copy files from the NIS+ client system to the DHCP client system by typing the following commands on the DHCP client system:**

```
# rcp nisplus-client-name:/var/nis/NIS_COLD_START /var/nis  
# rcp nisplus-client-name:/etc/.rootkey /etc  
# rcp nisplus-client-name:/etc/defaultdomain /etc
```

If you get a “permission denied” message, the systems might not be set up to allow remote copying. In this case, you can copy the files as a regular user to an intermediate location. As superuser, copy the files from the intermediate location to the proper location on the DHCP client system.

6. **Copy the correct name service switch file for NIS+ by typing the following command on the DHCP client system:**

```
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
```

7. **Reboot the DHCP client system.**

The DHCP client system should now be able to use NIS+ services.

Example 15–1 Setting up a Solaris DHCP Client System as an NIS+ Client

The following example assumes that you have one system `nisei`, which is an NIS+ client in the NIS+ domain `dev.example.net`. You also have one DHCP client system, `dhow`, and you want `dhow` to be an NIS+ client.

(First log in as superuser on the NIS+ server)

```
# nisgrep nisei cred.org_dir > /tmp/nisei-cred
```



```

# cat /tmp/nisei-cred
nisei.dev.example.net.:DES:unix.nisei@dev.example.net:46199279911a84045b8e0
c76822179138173a20edbd8eab4:90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830
c05bc1c724b
# nistbladm -a cname="dhow@dev.example.net." \
auth_type=DES auth_name="unix.dhow@dev.example.net" \
public_data=46199279911a84045b8e0c76822179138173a20edbd8eab4 \
private_data=90f2e2bb6ffe7e3547346dda624ec4c7f0fe1d5f37e21cff63830\
c05bc1c724b
# rlogin dhow
  (Log in as superuser on dhow)
# rcp nisei:/var/nis/NIS_COLD_START /var/nis
# rcp nisei:/etc/.rootkey /etc
# rcp nisei:/etc/defaultdomain /etc
# cp /etc/nsswitch.nisplus /etc/nsswitch.conf
# reboot

```

The DHCP client system dhow should now be able to use NIS+ services.

Example 15–2 Adding Credentials With a Script

If you want to set up a large number of DHCP client systems as NIS+ clients, you can write a script. A script can quickly add the entries to the `cred.org_dir` NIS+ table. The following example shows a sample script.

```

#!/usr/bin/ksh
#
# Copyright (c) by Sun Microsystems, Inc. All rights reserved.
#
# Sample script for cloning a credential. Hosts file is already populated
# with entries of the form dhcp-[0-9][0-9][0-9]. The entry we're cloning
# is dhcp-001.
#
#
PUBLIC_DATA=6e72878d8dc095a8b5aea951733d6ea91b4ec59e136bd3b3
PRIVATE_DATA=3a86729b685e2b2320cd7e26d4f1519ee070a60620a93e48a8682c5031058df4
HOST="dhcp-"
DOMAIN="mydomain.example.com"

for
i in 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019
do
    print - ${HOST}${i}
    #nistbladm -r [cname="${HOST}${i}.${DOMAIN}."]cred.org_dir
    nistbladm -a cname="${HOST}${i}.${DOMAIN}." \
        auth_type=DES auth_name="unix.${HOST}${i}@${DOMAIN}" \
        public_data=${PUBLIC_DATA} private_data=${PRIVATE_DTA} cred.org_dir
done

exit 0

```

DHCP Client Event Scripts

You can set up the Solaris DHCP client to run an executable program or script that can perform any action that is appropriate for the client system. The program or script, which is called an *event script*, is automatically executed after certain DHCP lease events occur. The event script can be used to run other commands, programs, or scripts in response to specific lease events. You must provide your own event script to use this feature.

The following event keywords are used by `dhcpcagent` to signify DHCP lease events:

Event Keyword	Description
BOUND	The interface is configured for DHCP. The client receives the acknowledgement message (ACK) from the DHCP server, which grants the lease request for an IP address. The event script is invoked immediately after the interface is configured successfully.
EXTEND	The client successfully extends a lease. The event script is invoked immediately after the client receives the acknowledgement message from the DHCP server for the renew request.
EXPIRE	The lease expires when the lease time is up. The event script is invoked immediately before the leased address is removed from the interface and the interface is marked as down.
DROP	The client drops the lease to remove the interface from DHCP control. The event script is invoked immediately before the interface is removed from DHCP control.
RELEASE	The client relinquishes the IP address. The event script is invoked immediately before the client releases the address on the interface and sends the RELEASE packet to the DHCP server.

With each of these events, `dhcpcagent` invokes the following command:

```
/etc/dhcp/eventhook interface event
```

where *interface* is the interface that is using DHCP and *event* is one of the event keywords described previously. For example, when the `ce0` interface is first configured for DHCP, the `dhcpcagent` invokes the event script as follows:

```
/etc/dhcp/eventhook ce0 BOUND
```

To use the event script feature, you must do the following:

- Name the executable file `/etc/dhcp/eventhook`.
- Set the owner of the file to be `root`.
- Set permissions to `755 (rwxr-xr-x)`.

- Write the script or program to perform a sequence of actions in response to any of the documented events. Because Sun might add new events, the program must silently ignore any events that are not recognized or do not require action. For example, the program or script might write to a log file when the event is `RELEASE`, and ignore all other events.
- Make the script or program noninteractive. Before the event script is invoked, `stdin`, `stdout`, and `stderr` are connected to `/dev/null`. To see the output or errors, you must redirect to a file.
- Enable the script or program to be run with the following command:

```
/etc/dhcp/eventhook interface event
```

The event script inherits its program environment from `dhcpcagent`, and runs with root privileges. The script can use the `dhcpinfo` utility to obtain more information about the interface, if necessary. See the `dhcpinfo(1)` man page for more information.

The `dhcpcagent` daemon waits for the event script to exit on all events. If the event script does not exit after 55 seconds, `dhcpcagent` sends a `SIGTERM` signal to the script process. If the process still does not exit after three additional seconds, the daemon sends a `SIGKILL` signal to kill the process.

The `dhcpcagent(1M)` man page includes one example of an event script.

Example 15-3 shows how to use a DHCP event script to keep the content of the `/etc/resolv.conf` file up to date. When the `BOUND` and `EXTEND` events occur, the script replaces the names of the domain server and name server. When the `EXPIRE`, `DROP` and `RELEASE` events occur, the script removes the names of the domain server and name server from the file.

Note – The example script assumes that DHCP is the authoritative source for the names of the domain server and the name server. The script also assumes that all interfaces under DHCP control return consistent and current information. These assumptions might not reflect conditions on your system.

EXAMPLE 15-3 Event Script for Updating the `/etc/resolv.conf` File

```
#!/bin/ksh -p

PATH=/bin:/sbin export PATH
umask 0222

# Refresh the domain and name servers on /etc/resolv.conf

insert ()
{
    dnsservers=`dhcpinfo -i $1 DNSserv`
    if [ -n "$dnsservers" ]; then
        # remove the old domain and name servers
```

EXAMPLE 15-3 Event Script for Updating the /etc/resolv.conf File (Continued)

```
if [ -f /etc/resolv.conf ]; then
    rm -f /tmp/resolv.conf.$$
    sed -e '/^domain/d' -e '/^nameserver/d' \
        /etc/resolv.conf > /tmp/resolv.conf.$$
fi

# add the new domain
dnsdomain=`dhcpcinfo -i $1 DNSdomain`
if [ -n "$dnsdomain" ]; then
    echo "domain $dnsdomain" >> /tmp/resolv.conf.$$
fi

# add new name servers
for name in $dnsservers; do
    echo nameserver $name >> /tmp/resolv.conf.$$
done
mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
fi
}

# Remove the domain and name servers from /etc/resolv.conf
remove ()
{
    if [ -f /etc/resolv.conf ]; then
        rm -f /tmp/resolv.conf.$$
        sed -e '/^domain/d' -e '/^nameserver/d' \
            /etc/resolv.conf > /tmp/resolv.conf.$$
        mv -f /tmp/resolv.conf.$$ /etc/resolv.conf
    fi
}

case $2 in
BOUND | EXTEND)
    insert $1
    exit 0
;;
EXPIRE | DROP | RELEASE)
    remove
    exit 0
;;
*)
    exit 0
;;
esac
```

Troubleshooting DHCP (Reference)

This chapter provides information to help you solve problems that you might encounter when you configure a DHCP server or client. The chapter also helps you with problems you might have in using DHCP after configuration is complete.

The chapter includes the following information:

- [“Troubleshooting DHCP Server Problems” on page 389](#)
- [“Troubleshooting DHCP Client Configuration Problems” on page 395](#)

See [Chapter 13](#) for information about configuring your DHCP server. See [“Enabling and Disabling a Solaris DHCP Client” on page 375](#) for information about configuring your DHCP client.

Troubleshooting DHCP Server Problems

The problems that you might encounter when you configure the server fall into the following categories:

- [“NIS+ Problems and the DHCP Data Store” on page 389](#)
- [“IP Address Allocation Errors in DHCP” on page 392](#)

NIS+ Problems and the DHCP Data Store

If you use NIS+ as the DHCP data store, problems that you might encounter can be categorized as follows:

- [“Cannot Select NIS+ as the DHCP Data Store” on page 390](#)
- [“NIS+ Is Not Adequately Configured for DHCP Data Store” on page 390](#)
- [“NIS+ Access Problems for the DHCP Data Store” on page 391](#)

Cannot Select NIS+ as the DHCP Data Store

If you try to use NIS+ as your data store, DHCP Manager might not offer NIS+ as a choice for the data store. If you use the `dhcpconfig` command, you might see a message stating that NIS+ does not appear to be installed and running. Both these symptoms mean that NIS+ has not been configured for this server, although NIS+ might be in use on the network. Before you can select NIS+ as a data store, the server system must be configured as an NIS+ client.

Before you set up the DHCP server system as an NIS+ client, the following statements must be true:

- The domain must have already been configured.
- The NIS+ domain's master server must be running.
- The master server's tables must be populated.
- The hosts table must have an entry for the new client system, the DHCP server system.

“Setting Up NIS+ Client Machines” in *System Administration Guide: Naming and Directory Services (NIS+)* provides detailed information about configuring an NIS+ client.

NIS+ Is Not Adequately Configured for DHCP Data Store

After you successfully use NIS+ with DHCP, you might encounter errors if changes are made to NIS+. The changes could introduce configuration problems. Use the following explanations of problems and solutions to help you determine the cause of configuration problems.

Problem: Root object does not exist in the NIS+ domain.

Solution: Type the following command:

```
/usr/lib/nis/nisstat
```

This command displays statistics for the domain. If the root object does not exist, no statistics are returned.

Set up the NIS+ domain using the *System Administration Guide: Naming and Directory Services (NIS+)*.

Problem: NIS+ is not used for `passwd` and `publickey` information.

Solution: Type the following command to view the configuration file for the name service switch:

```
cat /etc/nsswitch.conf
```

Check the `passwd` and `publickey` entries for the “nisplus” keyword. Refer to the *System Administration Guide: Naming and Directory Services (NIS+)* for information about configuring the name service switch.

Problem: The domain name is empty.

Solution: Type the following command:

```
domainname
```

If the command lists an empty string, no domain name has been set for the domain. Use local files for your data store, or set up an NIS+ domain for your network. Refer to the *System Administration Guide: Naming and Directory Services (NIS+)*.

Problem: The `NIS_COLD_START` file does not exist.

Solution: Type the following command on the server system to determine if the file exists:

```
cat /var/nis/NIS_COLD_START
```

Use local files for your data store, or create an NIS+ client. Refer to the *System Administration Guide: Naming and Directory Services (NIS+)*.

NIS+ Access Problems for the DHCP Data Store

NIS+ access problems might cause error messages about incorrect DES credentials, or inadequate permissions to update NIS+ objects or tables. Use the following explanations of problems and solutions to determine the cause of NIS+ access errors you receive.

Problem: The DHCP server system does not have create access to the `org_dir` object in the NIS+ domain.

Solution: Type the following command:

```
nisls -ld org_dir
```

The access rights are listed in the form `r---rmdrmdr---`, where the permissions apply respectively to nobody, owner, group, and world. The owner of the object is listed next.

Normally, the `org_dir` directory object provides full rights to both the owner and the group. Full rights consist of read, modify, create, and destroy. The `org_dir` directory object provides only read access to the world and nobody classes.

The DHCP server name must either be listed as the owner of the `org_dir` object, or be listed as a principal in the group. The group must have create access. List the group with the command:

```
nisls -ldg org_dir
```

Use the `nischmod` command to change the permissions for `org_dir` if necessary. For example, to add create access to the group, you would type the following command:

```
nischmod g+c org_dir
```

See the `nischmod(1)` man page for more information.

Problem: The DHCP server does not have access rights to create a table under the `org_dir` object.

Usually, this problem means the server system's principal name is not a member of the owning group for the `org_dir` object, or no owning group exists.

Solution: Type this command to find the owning group name:

```
niscat -o org_dir
```

Look for a line that is similar to:

```
Group : "admin.example.com."
```

List the principal names in the group using the command:

```
nisgrpadm -l groupname
```

For example, this command lists the principal names of the group

```
admin.example.com:
```

```
nisgrpadm -l admin.example.com
```

The server system's name should be listed as an explicit member of the group or included as an implicit member of the group. If necessary, add the server system's name to the group using the `nisgrpadm` command.

For example, to add the server name `pacific` to the group `admin.example.com`, you would type the following command:

```
nisgrpadm -a admin.example.com pacific.example.com
```

See the `nisgrpadm(1)` man page for more information.

Problem: The DHCP server does not have valid Data Encryption Standard (DES) credentials in the NIS+ `cred` table.

Solution: If there is a credential problem, an error message states that the user does not have DES credentials in the NIS+ name service.

Use the `nisaddcred` command to add security credentials for the DHCP server system.

The following example shows how to add DES credentials for the system `mercury` in the domain `example.com`:

```
nisaddcred -p unix.mercury@example.com \  
-P mercury.example.com. DES example.com.
```

The command prompts for the root password, which is required to generate an encrypted secret key.

See the `nisaddcred(1M)` man page for more information.

IP Address Allocation Errors in DHCP

When a client attempts to obtain or verify an IP address, you might see problems logged to `syslog` or in server debugging mode output. The following list of common error messages indicates the possible causes and solutions.

There is no *n.n.n.n* dhcp-network table for DHCP client's network

Cause: A client is requesting a specific IP address or seeking to extend a lease on its current IP address. The DHCP server cannot find the DHCP network table for that address.

Solution: The DHCP network table might have been deleted mistakenly. You can re-create the network table by adding the network again using DHCP Manager or the `dhcpconfig` command.

ICMP ECHO reply to OFFER candidate: *n.n.n.n*, disabling

Cause: The IP address considered for offering to a DHCP client is already in use. This problem might occur if more than one DHCP server owns the address. The problem might also occur if an address was manually configured for a non-DHCP network client.

Solution: Determine the proper ownership of the address. Correct either the DHCP server database or the host's network configuration.

ICMP ECHO reply to OFFER candidate: *n.n.n.n*. No corresponding dhcp network record.

Cause: The IP address considered for offering to a DHCP client does not have a record in a network table. This error indicates that the IP address record was deleted from the DHCP network table after the address was selected. This error can only happen in the brief period before the duplicate address check is completed.

Solution: Use DHCP Manager or the `pntadm` command to view the DHCP network table. If the IP address is missing, create the address with DHCP Manager by choosing Create from the Edit menu on the Address tab. You can also use `pntadm` to create the IP address.

DHCP network record for *n.n.n.n* is unavailable, ignoring request.

Cause: The record for the requested IP address is not in the DHCP network table, so the server is dropping the request.

Solution: Use DHCP Manager or the `pntadm` command to view the DHCP network table. If the IP address is missing, create the address with DHCP Manager by choosing Create from the Edit menu on the Address tab. You can also use `pntadm` to create the address.

n.n.n.n currently marked as unusable.

Cause: The requested IP address cannot be offered because the address has been marked in the network table as unusable.

Solution: You can use DHCP Manager or the `pntadm` command to make the address usable.

n.n.n.n was manually allocated. No dynamic address will be allocated.

Cause: The client ID has been assigned a manually allocated address, and that address is marked as unusable. The server cannot allocate a different address to this client.

Solution: You can use DHCP Manager or the `pntadm` command to make the address usable, or manually allocate a different address to the client.

Manual allocation (*n.n.n.n*, *client ID*) has *n* other records. Should have 0.

Cause: The client that has the specified client ID has been manually assigned more than one IP address. A client should be assigned only one address. The server selects the last manually assigned address that is found in the network table.

Solution: Use DHCP Manager or the `pntadm` command to modify IP addresses to remove the additional manual allocations.

No more IP addresses on *n.n.n.n* network.

Cause: All IP addresses currently managed by DHCP on the specified network have been allocated.

Solution: Use DHCP Manager or the `pntadm` command to create new IP addresses for this network.

Client: *clientid* lease on *n.n.n.n* expired.

Cause: The lease was not negotiable and timed out.

Solution: The client should automatically restart the protocol to obtain a new lease.

Offer expired for client: *n.n.n.n*

Cause: The server made an IP address offer to the client, but the client took too long to respond and the offer expired.

Solution: The client should automatically issue another discover message. If this message also times out, increase the cache offer timeout for the DHCP server. In DHCP Manager, choose Modify from the Service menu.

Client: *clientid* REQUEST is missing requested IP option.

Cause: The client's request did not specify the offered IP address, so the DHCP server ignored the request. This problem might occur if you use a third-party DHCP client that is not compliant with the updated DHCP protocol, RFC 2131.

Solution: Update the client software.

Client: *clientid* is trying to renew *n.n.n.n*, an IP address it has not leased.

Cause: The IP address for this client in the DHCP network table does not match the IP address that the client specified in its renewal request. The DHCP server does not renew the lease. This problem might occur if you delete a client's record while the client is still using the IP address.

Solution: Use DHCP Manager or the `pntadm` command to examine the network table, and correct the client's record, if necessary. The client ID should be bound to the specified IP address. If the client ID is not bound, edit the address properties to add the client ID.

Client: *clientid* is trying to verify unrecorded address: *n.n.n.n*, ignored.

Cause: The specified client has not been registered in the DHCP network table with this address, so the request is ignored by this DHCP server.

Another DHCP server on the network might have assigned this client the address. However, you might also have deleted the client's record while the client was still using the IP address.

Solution: Use DHCP Manager or the `pntadm` command to examine the network table on this server and any other DHCP servers on the network. Make corrections, if necessary.

You can also do nothing and allow the lease to expire. The client automatically requests a new address lease.

If you want the client to get a new lease immediately, restart the DHCP protocol on the client by typing the following commands:

```
ifconfig interface dhcp release
ifconfig interface dhcp start
```

Troubleshooting DHCP Client Configuration Problems

The problems that you might encounter with a DHCP client fall into the following categories:

- “Problems Communicating With the DHCP Server” on page 396
- “Problems With Inaccurate DHCP Configuration Information” on page 404

Problems Communicating With the DHCP Server

This section describes problems that you might encounter as you add DHCP clients to the network.

After you enable the client software and reboot the system, the client tries to reach the DHCP server to obtain its network configuration. If the client fails to reach the server, you might see error messages such as the following:

```
DHCP or BOOTP server not responding
```

Before you can determine the problem, you must gather diagnostic information from both the client and the server. To gather information, you can perform the following tasks:

1. [“How to Run the DHCP Client in Debugging Mode” on page 396](#)
2. [“How to Run the DHCP Server in Debugging Mode” on page 397](#)
3. [“How to Use snoop to Monitor DHCP Network Traffic” on page 397](#)

You can do these things separately or concurrently.

The information that you gather can help you determine if the problem is with the client, server, or a relay agent. Then, you can find a solution.

▼ How to Run the DHCP Client in Debugging Mode

If the client is not a Solaris DHCP client, refer to the client’s documentation for information about how to run the client in debugging mode.

If you have a Solaris DHCP client, use the following steps.

Steps 1. **Become superuser on the DHCP client system.**

2. **Kill the DHCP client daemon.**

```
# pkill -x dhcpcagent
```

3. **Restart the daemon in debugging mode.**

```
# /sbin/dhcpcagent -d1 -f &
```

The `-d` switch puts the DHCP client in debugging mode with level 1 verbosity. The `-f` switch causes output to be sent to the console instead of to `syslog`.

4. **Configure the interface to start DHCP negotiation.**

```
# ifconfig interface dhcp start
```

Replace *interface* with the name of the network interface of the client, such as `ge0`.

When run in debugging mode, the client daemon displays messages to your screen while performing DHCP requests. See [“Output from DHCP Client in Debugging Mode” on page 398](#) for information about client debugging mode output.

▼ How to Run the DHCP Server in Debugging Mode

Steps 1. Become superuser on the server system.

2. Stop the DHCP server temporarily.

```
# svcadm disable -t svc:/network/dhcp-server
```

You can also use DHCP Manager or `dhcpconfig` to stop the server.

3. Restart the daemon in debugging mode.

```
# /usr/lib/inet/in.dhcpd -d -v
```

You should also use any `in.dhcpd` command-line options that you normally use when you run the daemon. For example, if you run the daemon as a BOOTP relay agent, include the `-r` option with the `in.dhcpd -d -v` command.

When run in debugging mode, the daemon displays messages to your screen while processing DHCP or BOOTP requests. See [“Output from the DHCP Server in Debugging Mode” on page 398](#) for information about server debugging mode output.

▼ How to Use snoop to Monitor DHCP Network Traffic

Steps 1. Become superuser on the DHCP server system.

2. Start `snoop` to begin tracing network traffic across the server’s network interface.

```
# /usr/sbin/snoop -d interface -o snoop-output-filename udp port 67 or udp port 68
```

For example, you might type the following command:

```
# /usr/sbin/snoop -d hme0 -o /tmp/snoop.output udp port 67 or udp port 68
```

`snoop` continues to monitor the interface until you stop `snoop` by pressing Control-C after you have the information that you need.

3. Boot the client system, or restart the `dhcpcagent` on the client system.

[“How to Run the DHCP Client in Debugging Mode” on page 396](#) describes how to restart `dhcpcagent`.

4. On the server system, use `snoop` to display the output file with the contents of network packets:

```
# /usr/sbin/snoop -i snoop-output-filename -x0 -v
```

For example, you might type the following command:

```
# /usr/sbin/snoop -i /tmp/snoop.output -x0 -v
```

See Also See [“DHCP snoop Output” on page 401](#) for information about interpreting the output.

Output from DHCP Client in Debugging Mode

The following example shows normal output when a DHCP client in debugging mode sends its DHCP request and receives its configuration information from a DHCP server.

EXAMPLE 16-1 Normal Output from the DHCP Client in Debugging Mode

```
/sbin/dhclient: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhclient: debug: init_ifs: initted interface hme0
/sbin/dhclient: debug: insert_ifs: hme0: sdumax 1500, optmax 1260, hwtype 1, hwlen 6
/sbin/dhclient: debug: insert_ifs: inserted interface hme0
/sbin/dhclient: debug: register_acknak: registered acknak id 5
/sbin/dhclient: debug: unregister_acknak: unregistered acknak id 5
/sbin/dhclient: debug: set_packet_filter: set filter 0x26018 (ARP reply filter)
/sbin/dhclient: info: setting IP netmask on hme0 to 255.255.192.0
/sbin/dhclient: info: setting IP address on hme0 to 10.23.3.233
/sbin/dhclient: info: setting broadcast address on hme0 to 10.23.63.255
/sbin/dhclient: info: added default router 10.23.0.1 on hme0
/sbin/dhclient: debug: set_packet_filter: set filter 0x28054 (blackhole filter)
/sbin/dhclient: debug: configure_if: bound ifsp->if_sock_ip_fd
/sbin/dhclient: info: hme0 acquired lease, expires Tue Aug 10 16:18:33 2006
/sbin/dhclient: info: hme0 begins renewal at Tue Aug 10 15:49:44 2006
/sbin/dhclient: info: hme0 begins rebinding at Tue Aug 10 16:11:03 2006
```

If the client cannot reach the DHCP server, you might see debugging mode output that is similar to the output shown in the following example.

EXAMPLE 16-2 Output Indicating a Problem from the DHCP Client in Debugging Mode

```
/sbin/dhclient: debug: set_packet_filter: set filter 0x27fc8 (DHCP filter)
/sbin/dhclient: debug: init_ifs: initted interface hme0
/sbin/dhclient: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhclient: debug: select_best: no valid OFFER/BOOTP reply
/sbin/dhclient: debug: select_best: no valid OFFER/BOOTP reply
```

If you see this message, the client request never reached the server, or the server cannot send a response to the client. Run `snoop` on the server as described in [“How to Use snoop to Monitor DHCP Network Traffic”](#) on page 397 to determine if packets from the client have reached the server.

Output from the DHCP Server in Debugging Mode

Normal server debugging mode output shows server configuration information followed by information about each network interface as the daemon starts. After daemon startup, the debugging mode output shows information about requests the daemon processes. [Example 16-3](#) shows debugging mode output for a DHCP server that has just started. The server extends the lease for a client that is using an address owned by another DHCP server that is not responding.

EXAMPLE 16-3 Normal Output for DHCP Server in Debugging Mode

```
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
Run mode is: DHCP Server Mode.
Datastore: nisplus
Path: org_dir.dhcp.test...:dhcp.test...:$
DHCP offer TTL: 10
Ethers compatibility enabled.
BOOTP compatibility enabled.
ICMP validation timeout: 1000 milliseconds, Attempts: 2.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
Address: 10.23.0.1
Read 33 entries from DHCP macro database on Tue Aug 10 15:10:27 2006
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A is requesting verification of address owned by 10.21.0.4
Datagram received on network device: qfe0
Client: 0800201DBA3A maps to IP: 10.23.3.233
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
DHCP EXTEND 0934312543 0934316143 10.23.3.233 10.21.0.2
                0800201DBA3A SUNW.Ultra-5_10 0800201DBA3A
```

Example 16-4 shows debugging mode output from a DHCP daemon that starts as a BOOTP relay agent. The agent relays requests from a client to a DHCP server, and relays the server's responses to the client.

EXAMPLE 16-4 Normal Output from BOOTP Relay in Debugging Mode

```
Relay destination: 10.21.0.4 (blue-srvr2)      network: 10.21.0.0
Daemon Version: 3.1
Maximum relay hops: 4
Transaction logging to console enabled.
```

EXAMPLE 16-4 Normal Output from BOOTP Relay in Debugging Mode (Continued)

```
Run mode is: Relay Agent Mode.
Monitor (0005/hme0) started...
Thread Id: 0005 - Monitoring Interface: hme0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.21.255.255
Netmask: 255.255.0.0
Address: 10.21.0.2
Monitor (0006/nf0) started...
Thread Id: 0006 - Monitoring Interface: nf0 *****
MTU: 4352      Type: DLPI
Broadcast: 10.22.255.255
Netmask: 255.255.0.0
Address: 10.22.0.1
Monitor (0007/qfe0) started...
Thread Id: 0007 - Monitoring Interface: qfe0 *****
MTU: 1500      Type: DLPI
Broadcast: 10.23.63.255
Netmask: 255.255.192.0
Address: 10.23.0.1
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297685 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
BOOTP RELAY-CLNT 0934297688 0000000000 10.23.0.1 10.23.3.233 0800201DBA3A
N/A 0800201DBA3A
Relaying request 0800201DBA3A to 10.21.0.4, server port.
BOOTP RELAY-SRVR 0934297689 0000000000 0.0.0.0 10.21.0.4 0800201DBA3A
N/A 0800201DBA3A
Packet received from relay agent: 10.23.0.1
Relaying reply to client 0800201DBA3A
Unicasting datagram to 10.23.3.233 address.
Adding ARP entry: 10.23.3.233 == 0800201DBA3A
```

If there is a problem with DHCP, the debugging mode output might display warnings or error messages. Use the following list of DHCP server error messages to find solutions.

ICMP ECHO reply to OFFER candidate: *ip_address* disabling

Cause: Before the DHCP server offers an IP address to a client, the server pings the address to verify that the address is not in use. If a client replies, the address is in use.

Solution: Make sure the addresses that you configured are not already in use. You can use the ping command. See the ping(1M) man page for more information.

No more IP addresses on *network-address* network.

Cause: No IP addresses are available in the DHCP network table associated with the client's network.

Solution: Create more IP addresses with DHCP Manager or the `pntadm` command. If the DHCP daemon is monitoring multiple subnets, be sure the additional addresses are for the subnet where the client is located. See [“Adding IP Addresses to the DHCP Service” on page 328](#) for more information.

No more IP addresses for *network-address* network when you are running the DHCP daemon in BOOTP compatibility mode.

Cause: BOOTP does not use a lease time, so the DHCP server looks for free addresses with the BOOTP flag set to allocate to BOOTP clients.

Solution: Use DHCP Manager to allocate BOOTP addresses. See [“Supporting BOOTP Clients With the DHCP Service \(Task Map\)” on page 321](#).

Request to access nonexistent per network database: *database-name* in datastore: *datastore*.

Cause: During configuration of the DHCP server, a DHCP network table for a subnet was not created.

Solution: Use DHCP Manager or the `pntadm` command to create the DHCP network table and new IP addresses. See [“Adding DHCP Networks” on page 314](#).

There is no *table-name* dhcp-network table for DHCP client's network.

Cause: During configuration of the DHCP server, a DHCP network table for a subnet was not created.

Solution: Use DHCP Manager or the `pntadm` command to create the DHCP network table and new IP addresses. See [“Adding DHCP Networks” on page 314](#).

Client using non_RFC1048 BOOTP cookie.

Cause: A device on the network is trying to access an unsupported implementation of BOOTP.

Solution: Ignore this message, unless you need to configure this device. If you want to support the device, see [“Supporting BOOTP Clients With the DHCP Service \(Task Map\)” on page 321](#) for more information.

DHCP snoop Output

In the `snoop` output, you should see that packets are exchanged between the DHCP client system and the DHCP server system. The IP address for each system is indicated in each packet. IP addresses for any routers or relay agents in the packet's path are also included. If the systems do not exchange packets, the client system might not be able to contact the server system at all. The problem is then at a lower level.

To evaluate snoop output, you must know what the expected behavior is. For example, you must know if the request should be going through a BOOTP relay agent. You must also know the MAC addresses and the IP address of the systems involved so that you can determine if those values are as expected. If there is more than one network interface, you must know the addresses of the network interfaces as well.

The following example shows normal snoop output for a DHCP acknowledgement message sent from the DHCP server on `blue-srvr2` to a client whose MAC address is `8:0:20:8e:f3:7e`. In the message, the server assigns the client the IP address `192.168.252.6` and the host name `white-6`. The message also includes a number of standard network options and several vendor-specific options for the client.

EXAMPLE 16-5 Sample snoop Output for One Packet

```
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 26 arrived at 14:43:19.14
ETHER: Packet size = 540 bytes
ETHER: Destination = 8:0:20:8e:f3:7e, Sun
ETHER: Source      = 8:0:20:1e:31:c1, Sun
ETHER: Ethertype = 0800 (IP)
ETHER:
IP: ----- IP Header -----
IP:
IP: Version = 4
IP: Header length = 20 bytes
IP: Type of service = 0x00
IP:      xxx. .... = 0 (precedence)
IP:      ...0 .... = normal delay
IP:      .... 0... = normal throughput
IP:      .... .0.. = normal reliability
IP: Total length = 526 bytes
IP: Identification = 64667
IP: Flags = 0x4 IP:      .1.. .... = do not fragment
IP:      ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 254 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 157a
IP: Source address = 10.21.0.4, blue-srvr2
IP: Destination address = 192.168.252.6, white-6
IP: No options
IP: UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67
UDP: Destination port = 68 (BOOTPC)
UDP: Length = 506
UDP: Checksum = 5D4C
UDP:
DHCP: ----- Dynamic Host Configuration Protocol -----
DHCP:
DHCP: Hardware address type (htype) = 1 (Ethernet (10Mb))
DHCP: Hardware address length (hlen) = 6 octets
DHCP: Relay agent hops = 0
```

EXAMPLE 16-5 Sample snoop Output for One Packet (Continued)

```
DHCP: Transaction ID = 0x2e210f17
DHCP: Time since boot = 0 seconds
DHCP: Flags = 0x0000
DHCP: Client address (ciaddr) = 0.0.0.0
DHCP: Your client address (yiaddr) = 192.168.252.6
DHCP: Next server address (siaddr) = 10.21.0.2
DHCP: Relay agent address (giaddr) = 0.0.0.0
DHCP: Client hardware address (chaddr) = 08:00:20:11:E0:1B
DHCP:
DHCP: ----- (Options) field options -----
DHCP:
DHCP: Message type = DHCPACK
DHCP: DHCP Server Identifier = 10.21.0.4
DHCP: Subnet Mask = 255.255.255.0
DHCP: Router at = 192.168.252.1
DHCP: Broadcast Address = 192.168.252.255
DHCP: NISPLUS Domainname = dhcp.test
DHCP: IP Address Lease Time = 3600 seconds
DHCP: UTC Time Offset = -14400 seconds
DHCP: RFC868 Time Servers at = 10.21.0.4
DHCP: DNS Domain Name = sem.example.com
DHCP: DNS Servers at = 10.21.0.1
DHCP: Client Hostname = white-6
DHCP: Vendor-specific Options (166 total octets):
DHCP: (02) 04 octets 0x8194AE1B (unprintable)
DHCP: (03) 08 octets "pacific"
DHCP: (10) 04 octets 0x8194AE1B (unprintable)
DHCP: (11) 08 octets "pacific"
DHCP: (15) 05 octets "xterm"
DHCP: (04) 53 octets "/export/s2/base.s2s/latest/Solaris_8/Tools/Boot"
DHCP: (12) 32 octets "/export/s2/base.s2s/latest"
DHCP: (07) 27 octets "/platform/sun4u/kernel/unix"
DHCP: (08) 07 octets "EST5EDT"
  0: 0800 208e f37e 0800 201e 31c1 0800 4500  .. .6~.. .1...E.
 16: 020e fc9b 4000 fe11 157a ac15 0004 c0a8  ....@....z.....
 32: fc06 0043 0044 01fa 5d4c 0201 0600 2e21  ...C.D..]L.....!
 48: 0f17 0000 0000 0000 0000 c0a8 fc06 ac15  .....
 64: 0002 0000 0000 0800 2011 e01b 0000 0000  .....
 80: 0000 0000 0000 0000 0000 0000 0000 0000  .....
 96: 0000 0000 0000 0000 0000 0000 0000 0000  .....
112: 0000 0000 0000 0000 0000 0000 0000 0000  .....
128: 0000 0000 0000 0000 0000 0000 0000 0000  .....
144: 0000 0000 0000 0000 0000 0000 0000 0000  .....
160: 0000 0000 0000 0000 0000 0000 0000 0000  .....
176: 0000 0000 0000 0000 0000 0000 0000 0000  .....
192: 0000 0000 0000 0000 0000 0000 0000 0000  .....
208: 0000 0000 0000 0000 0000 0000 0000 0000  .....
224: 0000 0000 0000 0000 0000 0000 0000 0000  .....
240: 0000 0000 0000 0000 0000 0000 0000 0000  .....
256: 0000 0000 0000 0000 0000 0000 0000 0000  .....
272: 0000 0000 0000 6382 5363 3501 0536 04ac  .....c.Sc5..6..
288: 1500 0401 04ff ffff 0003 04c0 a8fc 011c  .....
304: 04c0 a8fc ff40 0964 6863 702e 7465 7374  ....@.dhcp.test
```

EXAMPLE 16-5 Sample snoop Output for One Packet (Continued)

```
320: 3304 0000 0e10 0204 ffff c7c0 0404 ac15 3.....
336: 0004 0f10 736e 742e 6561 7374 2e73 756e ....sem.example.
352: 2e63 6f6d 0604 ac15 0001 0c07 7768 6974 com.....whit
368: 652d 362b a602 0481 94ae 1b03 0861 746c e-6+.....pac
384: 616e 7469 630a 0481 94ae 1b0b 0861 746c ific.....pac
400: 616e 7469 630f 0578 7465 726d 0435 2f65 ific...xterm.5/e
416: 7870 6f72 742f 7332 382f 6261 7365 2e73 xport/sx2/bcvf.s
432: 3238 735f 776f 732f 6c61 7465 7374 2f53 2xs_btflatest/S
448: 6f6c 6172 6973 5f38 2f54 6f6f 6c73 2f42 olaris_x/Tools/B
464: 6f6f 740c 202f 6578 706f 7274 2f73 3238 oot. /export/s2x
480: 2f62 6173 652e 7332 3873 5f77 6f73 2f6c /bcvf.s2xs_btfl
496: 6174 6573 7407 1b2f 706c 6174 666f 726d atest../platform
512: 2f73 756e 346d 2f6b 6572 6e65 6c2f 756e /sun4u/kernel/un
528: 6978 0807 4553 5435 4544 54ff ix..EST5EDT.
```

Problems With Inaccurate DHCP Configuration Information

If a DHCP client receives inaccurate information in its network configuration information, look at the DHCP server data. You must examine the option values in the macros that the DHCP server processes for this client. Examples of inaccurate information might be the wrong NIS domain name or router IP address.

Use the following general guidelines to help you determine the source of the inaccurate information:

- Look at the macros defined on the server as described in [“How to View Macros Defined on a DHCP Server \(DHCP Manager\)”](#) on page 341. Review the information in [“Order of Macro Processing”](#) on page 260, and determine which macros are processed automatically for this client.
- Look at the network table to determine what macro (if any) is assigned to the client’s IP address as the configuration macro. See [“Working With IP Addresses in the DHCP Service \(Task Map\)”](#) on page 324 for more information.
- Take note of any options that occur in more than one macro. Make sure the value that you want for an option is set in the last processed macro.
- Edit the appropriate macro or macros to assure that the correct value is passed to the client. See [“Modifying DHCP Macros”](#) on page 342.

Problems With the DHCP Client-Supplied Host Name

This section describes problems that you might experience with DHCP clients that supply their own host names to be registered with DNS.

DHCP Client Does Not Request a Host Name

If your client is not a Solaris DHCP client, consult the client's documentation to determine how to configure the client to request a host name. For Solaris DHCP clients, see [“How to Enable a Solaris Client to Request a Specific Host Name”](#) on page 380.

DHCP Client Does Not Get Requested Host Name

The following list includes describes possible problems a client might have in getting its requested hostname, and suggested solutions.

Problem: Client accepted an offer from a DHCP server that does not issue DNS updates.

Solution: If two DHCP servers are available to the client, the servers should both be configured to provide DNS updates. See [“Enabling Dynamic DNS Updates by a DHCP Server”](#) on page 305 for information about configuring the DHCP server and the DNS server.

To determine whether the DHCP server is configured to provide DNS updates:

1. Determine the IP address of the client's DHCP server. On the client system, use `snoop` or another application for capturing network packets. See [“How to Use snoop to Monitor DHCP Network Traffic”](#) on page 397, and perform the procedure on the client instead of the server. In the `snoop` output, look for the DHCP Server Identifier to get the IP address of the server.
2. Log in to the DHCP server system to verify that the system is configured to make DNS updates. Type the following command as superuser:

```
dhcpcconfig -P
```

If `UPDATE_TIMEOUT` is listed as a server parameter, the DHCP server is configured to make DNS updates.
3. On the DNS server, look at the `/etc/named.conf` file. Find the `allow-update` keyword in the `zone` section of the appropriate domain. If the server allows DNS updates by the DHCP server, the DHCP server's IP address is listed in the `allow-update` keyword.

Problem: Client is using FQDN option to specify host name. Solaris DHCP does not currently support the FQDN option because the option is not officially in the DHCP protocol.

Solution: On the server, use `snoop` or another application for capturing network packets. See [“How to Use snoop to Monitor DHCP Network Traffic”](#) on page 397. In the `snoop` output, look for the FQDN option in a packet from the client.

Configure the client to specify host name using `Hostname` option. `Hostname` is option code 12. Refer to client documentation for instructions.

For a Solaris client, see [“How to Enable a Solaris Client to Request a Specific Host Name”](#) on page 380

Problem: DHCP server that makes an address offer to the client does not know the client's DNS domain.

Solution: On the DHCP server look for the `DNSdomain` option with a valid value. Set the `DNSdomain` option to the correct DNS domain name in a macro that is processed for this client. `DNSdomain` is usually contained in the network macro. See [“Modifying DHCP Macros” on page 342](#) for information about changing values of options in a macro.

Problem: The host name requested by client corresponds to an IP address that is not managed by the DHCP server. The Solaris DHCP server does not perform DNS updates for IP addresses that the server does not manage.

Solution: Check `syslog` for one of the following messages from the DHCP server:

- There is no `n.n.n.n dhcp-network` table for DHCP client's network.
- DHCP network record for `n.n.n.n` is unavailable, ignoring request.

Configure the client to request a different name. See [“How to Enable a Solaris Client to Request a Specific Host Name” on page 380](#). Choose a name that is mapped to an address managed by the DHCP server. You can see address mappings in DHCP Manager's Addresses tab. Alternatively, choose an address that is not mapped to any IP address.

Problem: The host name requested by client corresponds to an IP address that is currently not available for use. The address might be in use, leased to another client, or under offer to another client.

Solution: Check `syslog` for the following message from the DHCP server: `ICMP ECHO reply to OFFER candidate: n.n.n.n`.

Configure the client to choose a name corresponding to a different IP address. Alternatively, reclaim the address from the client that uses the address.

Problem: DNS server is not configured to accept updates from the DHCP server.

Solution: Examine the `/etc/named.conf` file on the DNS server. Look for the DHCP server's IP address with the `allow-update` keyword in the appropriate zone section for the DHCP server's domain. If the IP address is not present, the DNS server is not configured to accept updates from the DHCP server.

See [“How to Enable Dynamic DNS Updating for DHCP Clients” on page 306](#) for information about configuring the DNS server.

If the DHCP server has multiple interfaces, you might need to configure the DNS server to accept updates from all of the DHCP server's addresses. Enable debugging on the DNS server to see whether the updates are reaching the DNS server. If the DNS server received update requests, examine the debugging mode output to determine why the updates did not occur. See the `in.named(1M)` man page for information about DNS debugging mode.

Problem: DNS updates might not have completed in the allotted time. DHCP servers do not return host names to clients if the DNS updates have not completed by the configured time limit. However, attempts to complete the DNS updates continue.

Solution: Use the `nslookup` command to determine whether the updates completed successfully. See the `nslookup(1M)` man page.

For example, suppose the DNS domain is `hills.example.org`, and the DNS server's IP address is `10.76.178.11`. The host name that the client wants to register is `cathedral`. You could use the following command to determine if `cathedral` has been registered with that DNS server:

```
nslookup cathedral.hills.example.org 10.76.178.11
```

If the updates completed successfully, but not in the allotted time, you need to increase the timeout value. See [“How to Enable Dynamic DNS Updating for DHCP Clients” on page 306](#). In this procedure, you should increase the number of seconds to wait for a response from the DNS server before timing out.

DHCP Commands and Files (Reference)

This chapter explains the relationships between the DHCP commands and the DHCP files. However, the chapter does not explain how to use the commands.

The chapter contains the following information:

- “DHCP Commands” on page 409
- “Files Used by the DHCP Service” on page 416
- “DHCP Option Information” on page 418

DHCP Commands

The following table lists the commands that you can use to manage DHCP on your network.

TABLE 17-1 Commands Used in DHCP

Command	Description	Man Page
dhtadm	Used to make changes to the options and macros in the <code>dhcptab</code> . This command is most useful in scripts that you create to automate changes to your DHCP information. Use <code>dhtadm</code> with the <code>-P</code> option, and pipe the output through the <code>grep</code> command for a quick way to search for particular option values in the <code>dhcptab</code> table.	<code>dhtadm(1M)</code>
pntadm	Used to make changes to the DHCP network tables that map client IDs to IP addresses and optionally associate configuration information with IP addresses.	<code>pntadm(1M)</code>

TABLE 17-1 Commands Used in DHCP (Continued)

Command	Description	Man Page
<code>dhcpconfig</code>	Used to configure and unconfigure DHCP servers and BOOTP relay agents. Also used to convert to a different data store format, and to import and export DHCP configuration data.	<code>dhcpconfig(1M)</code>
<code>in.dhcpd</code>	The DHCP server daemon. The daemon is started when the system is started. You should not start the server daemon directly. Use DHCP Manager, the <code>svcadm</code> command, or <code>dhcpconfig</code> to start and stop the daemon. The daemon should be invoked directly only to run the server in debug mode to troubleshoot problems.	<code>in.dhcpd(1M)</code>
<code>dhcpcmgr</code>	The DHCP Manager, a graphical user interface (GUI) tool used to configure and manage the DHCP service. DHCP Manager is the recommended Solaris DHCP management tool.	<code>dhcpcmgr(1M)</code>
<code>ifconfig</code>	Used at system boot to assign IP addresses to network interfaces, configure network interface parameters, or both. On a Solaris DHCP client, <code>ifconfig</code> starts DHCP to get the parameters (including the IP address) needed to configure a network interface.	<code>ifconfig(1M)</code>
<code>dhcpinfo</code>	Used by system startup scripts on Solaris client systems to obtain information (such as the host name) from the DHCP client daemon, <code>dhcpcagent</code> . You can also use <code>dhcpinfo</code> in scripts or at the command line to obtain specified parameter values.	<code>dhcpinfo(1)</code>
<code>snoop</code>	Used to capture and display the contents of packets being passed across the network. <code>snoop</code> is useful for troubleshooting problems with the DHCP service.	<code>snoop(1M)</code>
<code>dhcpcagent</code>	The DHCP client daemon, which implements the client side of the DHCP protocol.	<code>dhcpcagent(1M)</code>

Running DHCP Commands in Scripts

The `dhcpconfig`, `dhtadm`, and `pntadm` commands are optimized for use in scripts. In particular, the `pntadm` command is useful for creating a large number of IP address entries in a DHCP network table. The following sample script uses `pntadm` in batch mode to create IP addresses.

EXAMPLE 17-1 `addclient.ksh` Script With the `pntadm` Command

```
#!/usr/bin/ksh
#
# This script utilizes the pntadm batch facility to add client entries
# to a DHCP network table. It assumes that the user has the rights to
```

EXAMPLE 17-1 addclient.ksh Script With the pntadm Command (Continued)

```
# run pntadm to add entries to DHCP network tables.

#
# Based on the nsswitch setting, query the netmasks table for a netmask.
# Accepts one argument, a dotted IP address.
#
get_netmask()
{
    MTMP=`getent netmasks ${1} | awk '{ print $2 }'`
    if [ ! -z "${MTMP}" ]
    then
        print - ${MTMP}
    fi
}

#
# Based on the network specification, determine whether or not network is
# subnetted or supernetted.
# Given a dotted IP network number, convert it to the default class
# network.(used to detect subnetting). Requires one argument, the
# network number. (e.g. 10.0.0.0) Echos the default network and default
# mask for success, null if error.
#
get_default_class()
{
    NN01=${1%%.*}
    tmp=${1#*.*}
    NN02=${tmp%%.*}
    tmp=${tmp#*.*}
    NN03=${tmp%%.*}
    tmp=${tmp#*.*}
    NN04=${tmp%%.*}
    RETNET=""
    RETMASK=""

    typeset -i16 ONE=10#${1%%.*}
    typeset -i10 X=$(( ${ONE} & 16#f0 ) )
    if [ ${X} -eq 224 ]
    then
        # Multicast
        typeset -i10 TMP=$(( ${ONE} & 16#f0 ) )
        RETNET="${TMP}.0.0.0"
        RETMASK="240.0.0.0"
    fi
    typeset -i10 X=$(( ${ONE} & 16#80 ) )
    if [ -z "${RETNET}" -a ${X} -eq 0 ]
    then
        # Class A
        RETNET="${NN01}.0.0.0"
        RETMASK="255.0.0.0"
    fi
    typeset -i10 X=$(( ${ONE} & 16#c0 ) )
    if [ -z "${RETNET}" -a ${X} -eq 128 ]
```

EXAMPLE 17-1 addclient.ksh Script With the pntadm Command (Continued)

```
then
    # Class B
    RETNET="${NN01}.${NN02}.0.0"
    RETMASK="255.255.0.0"
fi
typeset -i10 X=$(( ${ONE}&16#e0))
if [ -z "${RETNET}" -a $X -eq 192 ]
then
    # Class C
    RETNET="${NN01}.${NN02}.${NN03}.0"
    RETMASK="255.255.255.0"
fi
print - ${RETNET} ${RETMASK}
unset NNO1 NNO2 NNO3 NNO4 RETNET RETMASK X ONE
}

#
# Given a dotted form of an IP address, convert it to its hex equivalent.
#
convert_dotted_to_hex()
{
    typeset -i10 one=${1%%.*}
    typeset -i16 one=${one}
    typeset -Z2 one=${one}
    tmp=${1#*.*}

    typeset -i10 two=${tmp%%.*}
    typeset -i16 two=${two}
    typeset -Z2 two=${two}
    tmp=${tmp#*.*}

    typeset -i10 three=${tmp%%.*}
    typeset -i16 three=${three}
    typeset -Z2 three=${three}
    tmp=${tmp#*.*}

    typeset -i10 four=${tmp%%.*}
    typeset -i16 four=${four}
    typeset -Z2 four=${four}

    hex=`print - ${one}${two}${three}${four} | sed -e 's/#/0/g'`
    print - 16#${hex}
    unset one two three four tmp
}

#
# Generate an IP address given the network address, mask, increment.
#
get_addr()
{
    typeset -i16 net=`convert_dotted_to_hex ${1}`
    typeset -i16 mask=`convert_dotted_to_hex ${2}`
    typeset -i16 incr=10#${3}
}
```

EXAMPLE 17-1 addclient.ksh Script With the pntadm Command (Continued)

```
# Maximum legal value - invert the mask, add to net.
typeset -i16 mhosts=~${mask}
typeset -i16 maxnet=${net}+${mhosts}

# Add the incr value.
let net=${net}+${incr}

if [ ${net} < ${maxnet} ] -eq 1 ]
then
    typeset -i16 a=${net}\&16#ff00000
    typeset -i10 a="${a}>>24"

    typeset -i16 b=${net}\&16#ff0000
    typeset -i10 b="${b}>>16"

    typeset -i16 c=${net}\&16#ff00
    typeset -i10 c="${c}>>8"

    typeset -i10 d=${net}\&16#ff
    print - "${a}.${b}.${c}.${d}"
fi
unset net mask incr mhosts maxnet a b c d
}

# Given a network address and client address, return the index.
client_index()
{
    typeset -i NNO1=${1%.*}
    tmp=${1#*.*}
    typeset -i NNO2=${tmp%.*}
    tmp=${tmp#*.*}
    typeset -i NNO3=${tmp%.*}
    tmp=${tmp#*.*}
    typeset -i NNO4=${tmp%.*}

    typeset -i16 NNF1
    let NNF1=${NNO1}
    typeset -i16 NNF2
    let NNF2=${NNO2}
    typeset -i16 NNF3
    let NNF3=${NNO3}
    typeset -i16 NNF4
    let NNF4=${NNO4}
    typeset +i16 NNF1
    typeset +i16 NNF2
    typeset +i16 NNF3
    typeset +i16 NNF4
    NNF1=${NNF1#16\#}
    NNF2=${NNF2#16\#}
    NNF3=${NNF3#16\#}
    NNF4=${NNF4#16\#}
    if [ ${#NNF1} -eq 1 ]
```

EXAMPLE 17-1 addclient.ksh Script With the pntadm Command (Continued)

```
then
    NNF1="0${NNF1}"
fi
if [ ${#NNF2} -eq 1 ]
then
    NNF2="0${NNF2}"
fi
if [ ${#NNF3} -eq 1 ]
then
    NNF3="0${NNF3}"
fi
if [ ${#NNF4} -eq 1 ]
then
    NNF4="0${NNF4}"
fi
typeset -i16 NN
let NN=16#${NNF1}${NNF2}${NNF3}${NNF4}
unset NNF1 NNF2 NNF3 NNF4

typeset -i NNO1=${2%%.*}
tmp=${2#*.*}
typeset -i NNO2=${tmp%%.*}
tmp=${tmp#*.*}
typeset -i NNO3=${tmp%%.*}
tmp=${tmp#*.*}
typeset -i NNO4=${tmp%%.*}
typeset -i16 NNF1
let NNF1=${NNO1}
typeset -i16 NNF2
let NNF2=${NNO2}
typeset -i16 NNF3
let NNF3=${NNO3}
typeset -i16 NNF4
let NNF4=${NNO4}
typeset +i16 NNF1
typeset +i16 NNF2
typeset +i16 NNF3
typeset +i16 NNF4
NNF1=${NNF1#16\#}
NNF2=${NNF2#16\#}
NNF3=${NNF3#16\#}
NNF4=${NNF4#16\#}
if [ ${#NNF1} -eq 1 ]
then
    NNF1="0${NNF1}"
fi
if [ ${#NNF2} -eq 1 ]
then
    NNF2="0${NNF2}"
fi
if [ ${#NNF3} -eq 1 ]
then
    NNF3="0${NNF3}"
```

EXAMPLE 17-1 addclient.ksh Script With the pntadm Command (Continued)

```
fi
if [ $#{#NNF4} -eq 1 ]
then
    NNF4="0${NNF4}"
fi
typeset -i16 NC
let NC=16#${NNF1}${NNF2}${NNF3}${NNF4}
typeset -i10 ANS
let ANS=${NC}-${NN}
print - $ANS
}

#
# Check usage.
#
if [ "$#" != 3 ]
then
    print "This script is used to add client entries to a DHCP network"
    print "table by utilizing the pntadm batch facility.\n"
    print "usage: $0 network start_ip entries\n"
    print "where: network is the IP address of the network"
        print "        start_ip is the starting IP address \n"
        print "        entries is the number of the entries to add\n"
    print "example: $0 10.148.174.0 10.148.174.1 254\n"
    return
fi

#
# Use input arguments to set script variables.
#
NETWORK=$1
START_IP=$2
typeset -i STRTNUM='client_index ${NETWORK} ${START_IP}'
let ENDRNUM=${STRTNUM}+3
let ENTRYNUM=${STRTNUM}
BATCHFILE=/tmp/batchfile.$$
MACRO='uname -n'

#
# Check if mask in netmasks table. First try
# for network address as given, in case VLSM
# is in use.
#
NETMASK='get_netmask ${NETWORK}'
if [ -z "${NETMASK}" ]
then
    get_default_class ${NETWORK} | read DEFNET DEFMASK
    # use the default.
    if [ "${DEFNET}" != "${NETWORK}" ]
    then
        # likely subnetted/supernetted.
        print - "\n\n###\tWarning\t###\n"
        print - "Network ${NETWORK} is netmasked, but no entry was found \n"
    fi
fi
```

EXAMPLE 17-1 addclient.ksh Script With the pntadm Command (Continued)

```
        in the 'netmasks' table; please update the 'netmasks' \n
        table in the appropriate nameservice before continuing. \n
        (See /etc/nsswitch.conf.) \n" >&2
    return 1
else
    # use the default.
    NETMASK="${DEFMASK}"
fi
fi

#
# Create a batch file.
#
print -n "Creating batch file "
while [ ${ENTRYNUM} -lt ${ENDNUM} ]
do
    if [ (($({ENTRYNUM}-${STRTNUM}))%50 -eq 0 )
    then
        print -n "."
    fi

    CLIENTIP=`get_addr ${NETWORK} ${NETMASK} ${ENTRYNUM}`
    print "pntadm -A ${CLIENTIP} -m ${MACRO} ${NETWORK}" >> ${BATCHFILE}
    let ENTRYNUM=${ENTRYNUM}+1
done
print " done.\n"

#
# Run pntadm in batch mode and redirect output to a temporary file.
# Progress can be monitored by using the output file.
#
print "Batch processing output redirected to ${BATCHFILE}"
print "Batch processing started."

pntadm -B ${BATCHFILE} -v > /tmp/batch.out 2 >&1

print "Batch processing completed."
```

Files Used by the DHCP Service

The following table lists files associated with Solaris DHCP.

TABLE 17-2 Files and Tables Used by DHCP Daemons and Commands

File or Table Name	Description	Man Page
dhcptab	A generic term for the table of DHCP configuration information that is recorded as options with assigned values, which are then grouped into macros. The name of the <code>dhcptab</code> table and its location is determined by the data store you use for DHCP information.	dhcptab(4)
DHCP network table	Maps IP addresses to client IDs and configuration options. DHCP network tables are named according to the IP address of the network, such as <code>10.21.32.0</code> . There is no file that is called <code>dhcp_network</code> . The name and location of DHCP network tables is determined by the data store you use for DHCP information.	dhcp_network(4)
dhcpsvc.conf	Stores startup options for the DHCP daemon and data store information. This file must not be edited manually. Use the <code>dhcpconfig</code> command to change startup options.	dhcpsvc.conf(4)
nsswitch.conf	Specifies the location of name service databases and the order in which to search name services for various kinds of information. The <code>nsswitch.conf</code> file is read to obtain accurate configuration information when you configure a DHCP server. The file is located in the <code>/etc</code> directory.	nsswitch.conf(4)
resolv.conf	Contains information used to resolve DNS queries. During DHCP server configuration, this file is consulted for information about the DNS domain and DNS server. The file is located in the <code>/etc</code> directory.	resolv.conf(4)
dhcp.interface	Indicates that DHCP is to be used on the client's network interface that is specified in the <code>dhcp.interface</code> file name. For example, the existence of a file named <code>dhcp.qe0</code> indicates that DHCP is to be used on the <code>qe0</code> interface. The <code>dhcp.interface</code> file might contain commands that are passed as options to the <code>ifconfig</code> command, which is used to start DHCP on the client. The file is located in the <code>/etc</code> directory on Solaris DHCP client systems.	No specific man page, see dhcp(5)

TABLE 17-2 Files and Tables Used by DHCP Daemons and Commands (Continued)

File or Table Name	Description	Man Page
<i>interface</i> .dnc	Contains the configuration parameters that are obtained from DHCP for the given network interface. The client caches the current configuration information in <code>/etc/dhcp/interface.dnc</code> when the interface's IP address lease is dropped. For example, if DHCP is used on the <code>qe0</code> interface, the <code>dhcpagent</code> caches the configuration information in <code>/etc/dhcp/qe0.dnc</code> . The next time DHCP starts on the interface, the client requests to use the cached configuration if the lease has not expired. If the DHCP server denies the request, the client begins the standard process for DHCP lease negotiation.	No specific man page, see <code>dhcpagent(1M)</code>
<code>dhcpagent</code>	Sets parameter values for the <code>dhcpagent</code> client daemon. The path to the file is <code>/etc/default/dhcpagent</code> . See the <code>/etc/default/dhcpagent</code> file or the <code>dhcpagent(1M)</code> man page for information about the parameters.	<code>dhcpagent(1M)</code>
DHCP <code>inittab</code>	Defines aspects of DHCP option codes, such as the data type, and assigns mnemonic labels. See the <code>dhcp_inittab(4)</code> man page for more information about the file syntax. On the client, the information in the <code>/etc/dhcp/inittab</code> file is used by <code>dhcpinfo</code> to provide more meaningful information to human readers of the information. On the DHCP server system, this file is used by the DHCP daemon and management tools to obtain DHCP option information. The <code>/etc/dhcp/inittab</code> file replaces the <code>/etc/dhcp/dhcptags</code> file that was used in previous releases. “ DHCP Option Information ” on page 418 provides more information about this replacement.	<code>dhcp_inittab(4)</code>

DHCP Option Information

Historically, DHCP option information has been stored in several places, including the server's `dhcptab` table, the client's `dhcptags` file, and internal tables of various programs. In the Solaris 8 release and later releases, the option information is consolidated in the `/etc/dhcp/inittab` file. See the `dhcp_inittab(4)` man page for detailed information about the file.

The Solaris DHCP client uses the DHCP `inittab` file as a replacement for the `dhcptags` file. The client uses the file to obtain information about option codes that were received in a DHCP packet. The `in.dhcpd`, `snoop`, and `dhcpcmgr` programs on the DHCP server use the `inittab` file as well.

Determining if Your Site Is Affected

Most sites that use Solaris DHCP are *not* affected by the switch to the `/etc/dhcp/inittab` file. Your site is affected if you meet all of the following criteria:

- You plan to upgrade from a Solaris release that is older than that the Solaris 8 release.
- You previously created new DHCP options.
- You modified the `/etc/dhcp/dhcptags` file, and you want to retain the changes.

When you upgrade, the upgrade log notifies you that your `dhcptags` file had been modified and that you should make changes to the DHCP `inittab` file.

Differences Between `dhcptags` and `inittab` Files

The `inittab` file contains more information than the `dhcptags` file. The `inittab` file also uses a different syntax.

A sample `dhcptags` entry is as follows:

```
33 StaticRt - IPList Static_Routes
```

33 is the numeric code that is passed in the DHCP packet. `StaticRt` is the option name. `IPList` indicates that the data type for `StaticRt` must be a list of IP addresses. `Static_Routes` is a more descriptive name.

The `inittab` file consists of one-line records that describe each option. The format is similar to the format that defines symbols in `dhcptab`. The following table describes the syntax of the `inittab` file.

Option	Description
<i>option-name</i>	Name of the option. The option name must be unique within its option category, and not overlap with other option names in the Standard, Site, and Vendor categories. For example, you cannot have two Site options with the same name, and you should not create a Site option with the same name as a Standard option.
<i>category</i>	Identifies the namespace in which the option belongs. Must be one of the following: Standard, Site, Vendor, Field, or Internal.

<i>code</i>	Identifies the option when sent over the network. In most cases, the code uniquely identifies the option, without a category. However, in the case of internal categories such as Field or Internal, a code might be used for other purposes. The code might not be globally unique. The code should be unique within the option's category, and not overlap with codes in the Standard and Site fields.
<i>type</i>	Describes the data that is associated with this option. Valid types are IP, Ascii, Octet, Boolean, Unumber8, Unumber16, Unumber32, Unumber64, Snumber8, Snumber16, Snumber32, and Snumber64. For numbers, an initial U or S indicates that the number is unsigned or signed. The digits at the end indicate how many bits are in the number. For example, Unumber8 is an unsigned 8-bit number. The type is not case sensitive.
<i>granularity</i>	Describes how many units of data make up a whole value for this option.
<i>maximum</i>	Describes how many whole values are allowed for this option. 0 indicates an infinite number.
<i>consumers</i>	Describes which programs can use this information. Consumers should be set to <i>sdmi</i> , where: <ul style="list-style-type: none"> s snoop d in.dhcpd m dhcpmgr i dhcpinfo

A sample *inittab* entry is as follows:

```
StaticRt - Standard, 33, IP, 2, 0, sdmi
```

This entry describes an option that is named *StaticRt*. The option is in the Standard category, and is option code 33. The expected data is a potentially infinite number of pairs of IP addresses because the type is *IP*, the granularity is 2, and the maximum is infinite (0). The consumers of this option are *sdmi*: *snoop*, *in.dhcpd*, *dhcpmgr*, and *dhcpinfo*.

Converting `dhcptags` Entries to `inittab` Entries

If you previously added entries to your `dhcptags` file, you must add corresponding entries to the new `inittab` file if you want to continue using the options you added to your site. The following example shows how a sample `dhcptags` entry might be expressed in `inittab` format.

Suppose you had added the following `dhcptags` entry for fax machines that are connected to the network:

```
128 FaxMchn - IP Fax_Machine
```

The code `128` means that the option must be in the Site category. The option name is `FaxMchn`, and the data type is `IP`.

The corresponding `inittab` entry might be:

```
FaxMchn SITE, 128, IP, 1, 1, sdmi
```

The granularity of `1` and the maximum of `1` indicate that one IP address is expected for this option.

PART **IV** IP Security

This section focuses on network security. IP security architecture (IPsec) protects the network at the packet level. Internet key management (IKE) manages the keys for IPsec. Solaris IP filter provides a firewall.

IP Security Architecture (Overview)

The IP Security Architecture (IPsec) provides cryptographic protection for IP datagrams in IPv4 and IPv6 network packets.

This chapter contains the following information:

- “Introduction to IPsec” on page 425
- “IPsec Packet Flow” on page 428
- “IPsec Security Associations” on page 431
- “IPsec Protection Mechanisms” on page 432
- “IPsec Protection Policies” on page 434
- “Transport and Tunnel Modes in IPsec” on page 435
- “Virtual Private Networks and IPsec” on page 436
- “IPsec and NAT Traversal” on page 437
- “IPsec and SCTP” on page 438
- “IPsec and Solaris Zones” on page 439
- “IPsec Utilities and Files” on page 439
- “Changes to IPsec for the Solaris 10 Release” on page 440

To implement IPsec on your network, see [Chapter 19](#). For reference information, see [Chapter 20](#).

Introduction to IPsec

IPsec protects IP packets by authenticating the packets, by encrypting the packets, or by doing both. IPsec is performed inside the IP module, well below the application layer. Therefore, an Internet application can take advantage of IPsec while not having to configure itself to use IPsec. When used properly, IPsec is an effective tool in securing network traffic.

IPsec protection involves five main components:

- **Security protocols** – The IP datagram protection mechanisms. The [authentication header \(AH\)](#) signs IP packets and ensures integrity. The content of the datagram is not encrypted, but the receiver is assured that the packet contents have not been altered. The receiver is also assured that the packets were sent by the sender. The [encapsulating security payload \(ESP\)](#) encrypts IP data, thus obscuring the content during packet transmission. ESP also can ensure data integrity through an authentication algorithm option.
- **Security associations database (SADB)** – The database that associates a security protocol with an IP destination address and an indexing number. The indexing number is called the [security parameter index \(SPI\)](#). These three elements (the security protocol, the destination address, and the SPI) uniquely identify a legitimate IPsec packet. The database ensures that a protected packet that arrives to the packet destination is recognized by the receiver. The receiver also uses information from the database to decrypt the communication, verify that the packets are unchanged, reassemble the packets, and deliver the packets to their ultimate destination.
- **Key management** – The generation and distribution of keys for the cryptographic algorithms and for the SPI.
- **Security mechanisms** – The authentication and encryption algorithms that protect the data in the IP datagrams.
- **Security policy database (SPD)** – The database that specifies the level of protection to apply to a packet. The SPD filters IP traffic to determine how the packets should be processed. A packet can be discarded. A packet can be passed in the clear. Or, a packet can be protected with IPsec. For outbound packets, the SPD and the SADB determine what level of protection to apply. For inbound packets, the SPD helps to determine if the level of protection on the packet is acceptable. If the packet is protected by IPsec, the SPD is consulted after the packet has been decrypted and has been verified.

When you invoke IPsec, IPsec applies the security mechanisms to IP datagrams that travel to the IP destination address. The receiver uses information in its SADB to verify that the arriving packets are legitimate, and to decrypt them. Applications can invoke IPsec to apply security mechanisms to IP datagrams on a per-socket level as well. Note that sockets behave differently from ports:

- Per-socket SAs override their corresponding port entry in the SPD.
- Also, if a socket on a port is connected, and IPsec policy is later applied to that port, then traffic that uses that socket is not protected by IPsec.
Of course, a socket that is opened on a port *after* IPsec policy is applied to the port is protected by IPsec policy.

IPsec RFCs

The Internet Engineering Task Force (IETF) has published a number of Requests for Comment (RFCs) that describe the security architecture for the IP layer. All RFCs are copyrighted by the Internet Society. For a link to the RFCs, see <http://ietf.org/>. The following list of RFCs covers the more general IP security references:

- RFC 2411, "IP Security Document Roadmap," November 1998
- RFC 2401, "Security Architecture for the Internet Protocol," November 1998
- RFC 2402, "IP Authentication Header," November 1998
- RFC 2406, "IP Encapsulating Security Payload (ESP)," November 1998
- RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)," November 1998
- RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP," November 1998
- RFC 2409, "The Internet Key Exchange (IKE)," November 1998
- RFC 3554, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec," July 2003 [not implemented in the Solaris 10 release]

IPsec Terminology

The IPsec RFCs define a number of terms that are useful to recognize when implementing IPsec on your systems. The following table lists IPsec terms, provides their commonly used acronyms, and defines each term. For a list of terminology used in key negotiation, see [Table 21-1](#).

TABLE 18-1 IPsec Terms, Acronyms, and Uses

IPsec Term	Acronym	Definition
Security association	SA	A unique connection between two nodes on a network. The connection is defined by a triplet: a security protocol, a security parameter index, and an IP destination. The IP destination can be an IP address or a socket.
Security associations database	SADB	Database that contains all active security associations.
Security parameter index	SPI	The indexing value for a security association. An SPI is a 32-bit value that distinguishes among SAs that have the same IP destination and security protocol.
Security policy database	SPD	Database that determines if outbound packets and inbound packets have the specified level of protection.

TABLE 18-1 IPsec Terms, Acronyms, and Uses (Continued)

IPsec Term	Acronym	Definition
Key exchange		The process of generating keys for asymmetric cryptographic algorithms. The two main methods are RSA protocols and the Diffie-Hellman protocol.
Diffie-Hellman protocol	DH	A key exchange protocol that involves key generation and key authentication. Often called <i>authenticated key exchange</i> .
RSA protocol	RSA	A key exchange protocol that involves key generation and key distribution. The protocol is named for its three creators, Rivest, Shamir, and Adleman.
Internet Security Association and Key Management Protocol	ISAKMP	The common framework for establishing the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP is the IETF standard for handling IPsec SAs.

IPsec Packet Flow

Figure 18-1 shows how an IP addressed packet, as part of an IP datagram, proceeds when IPsec has been invoked on an outbound packet. The flow diagram illustrates where authentication header (AH) and encapsulating security payload (ESP) entities can be applied to the packet. How to apply these entities, as well as how to choose the algorithms, are described in subsequent sections.

Figure 18-2 shows the IPsec inbound process.

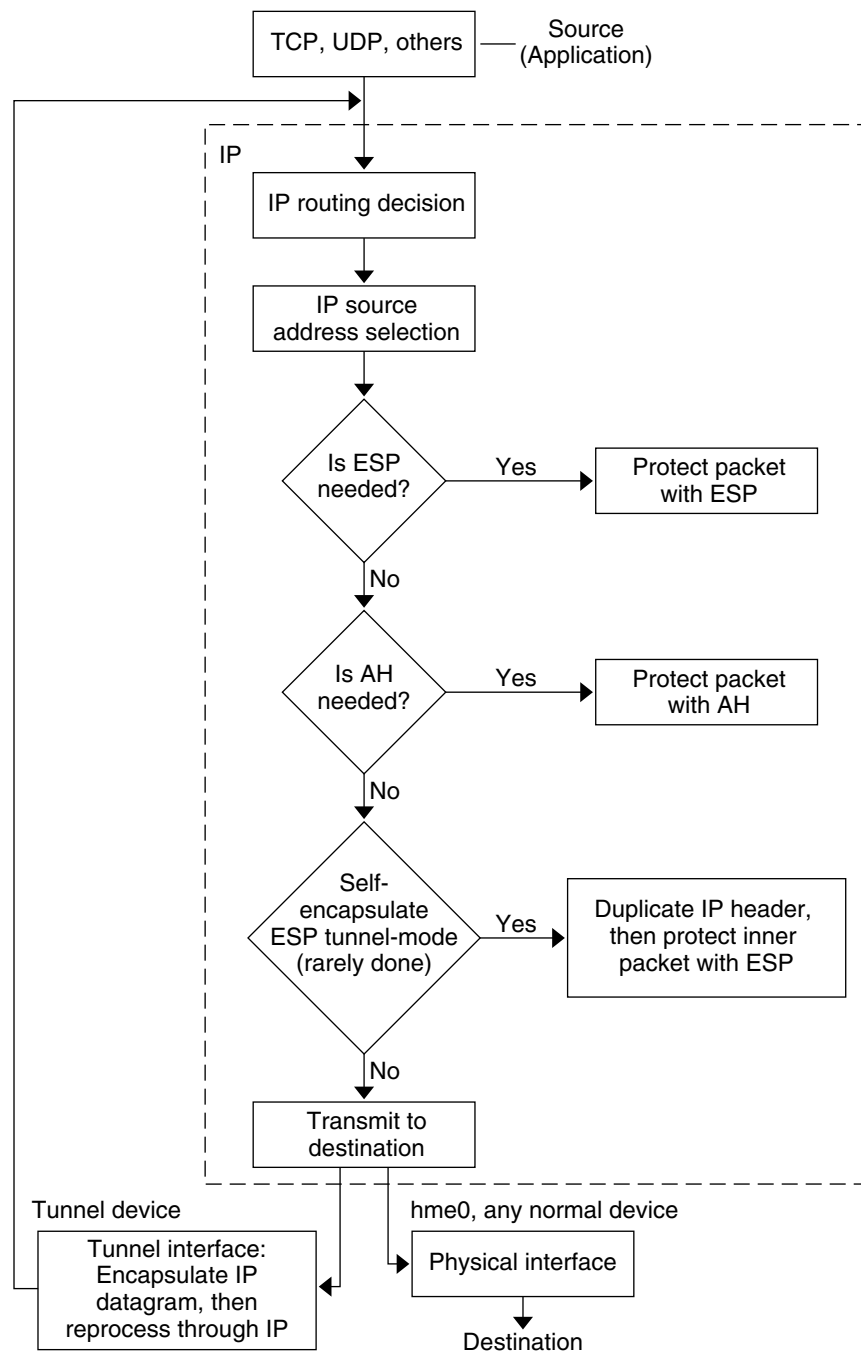


FIGURE 18-1 IPsec Applied to Outbound Packet Process

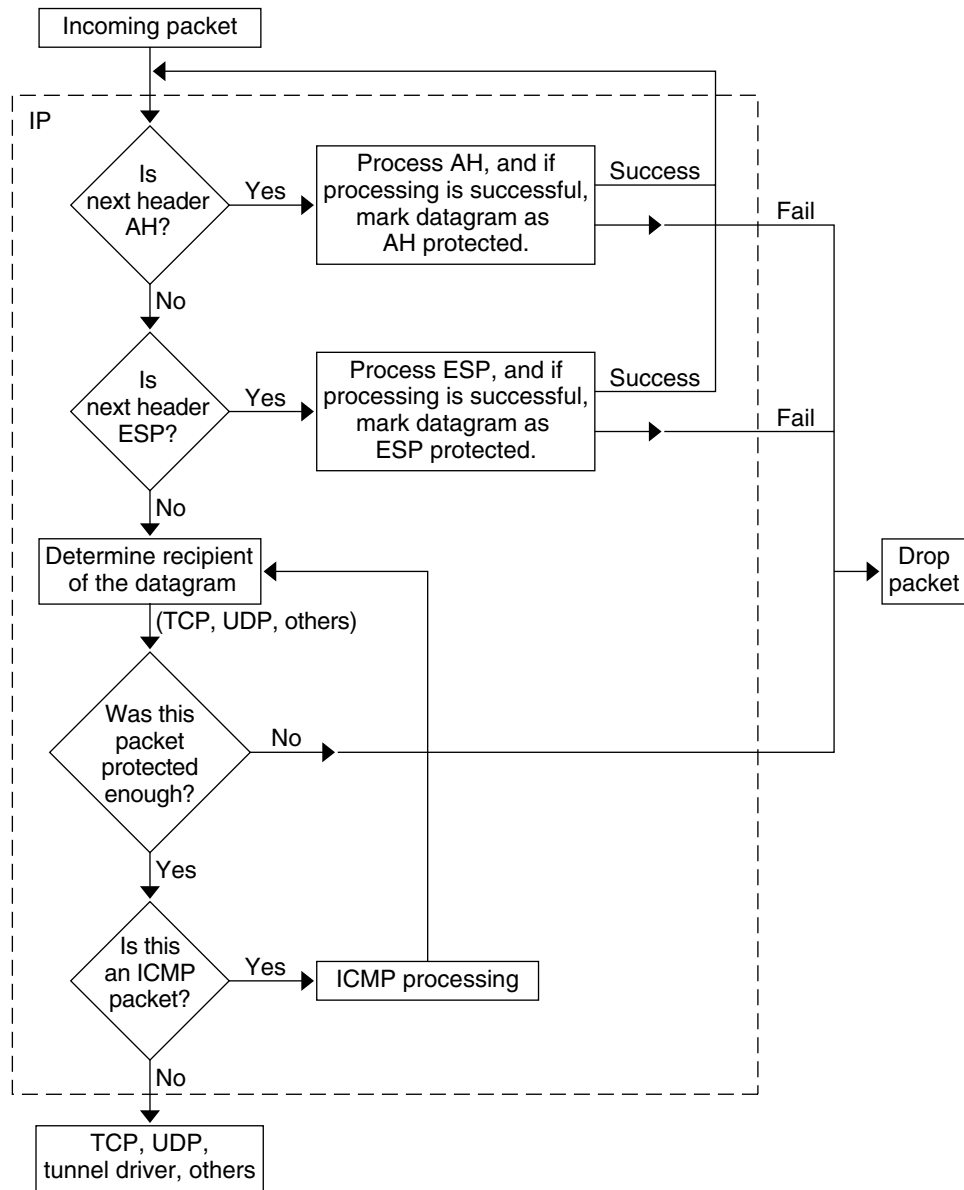


FIGURE 18-2 IPsec Applied to Inbound Packet Process

IPsec Security Associations

An IPsec *security association* (SA) specifies security properties that are recognized by communicating hosts. A single SA protects data in one direction. The protection is either to a single host or to a group (multicast) address. Because most communication is either peer-to-peer or client-server, two SAs must be present to secure traffic in both directions.

The following three elements uniquely identify an IPsec SA:

- The security protocol (AH or ESP)
- The destination IP address
- The [security parameter index \(SPI\)](#)

The SPI, an arbitrary 32-bit value, is transmitted with an AH or ESP packet. The `ipsecah(7P)` and `ipsecesp(7P)` man pages explain the extent of protection that is provided by AH and ESP. An integrity checksum value is used to authenticate a packet. If the authentication fails, the packet is dropped.

Security associations are stored in a *security associations database* (SADB). A socket-based administration engine, the `pf_key` interface, enables privileged applications to manage the database.

- For a more complete description of the IPsec SADB, see [“Security Associations Database for IPsec”](#) on page 472.
- For more information about how to manage the SADB, see the `pf_key(7P)` man page.

Key Management in IPsec

Security associations (SAs) require material to create the keys for authentication and for encryption. The managing of this *keying material* is called *key management*. The Internet Key Exchange (IKE) protocol handles key management automatically. You can also manage keys manually with the `ipseckey` command.

SAs on IPv4 and IPv6 packets can use either method of key management. Unless you have an overriding reason to use manual key management, automatic key management is preferred. For example, to interoperate with systems other than Solaris systems might require manual key management.

- The `in.iked` daemon provides automatic key management. For a description of IKE, see [Chapter 21](#). For more information on the `in.iked` daemon, see the `in.iked(1M)` man page.
- The `ipseckey` command provides manual key management. For a description of the command, see [“Utilities for Key Generation in IPsec”](#) on page 473. For a detailed description of the `ipseckey` command options, see the `ipseckey(1M)`

man page.

IPsec Protection Mechanisms

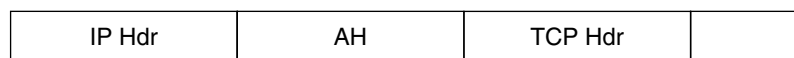
IPsec provides two security protocols for protecting data:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

An AH protects data with an authentication algorithm. An ESP protects data with an encryption algorithm. Optionally, an ESP protects data with an authentication algorithm. Each implementation of an algorithm is called a *mechanism*.

Authentication Header

The [authentication header](#) provides data authentication, strong integrity, and replay protection to IP datagrams. AH protects the greater part of the IP datagram. As the following illustration shows, AH is inserted between the IP header and the transport header.



The transport header can be TCP, UDP, SCTP, or ICMP. If a [tunnel](#) is being used, the transport header can be another IP header.

Encapsulating Security Payload

The [encapsulating security payload \(ESP\)](#) module provides confidentiality over what the ESP encapsulates. ESP also provides the services that AH provides. However, ESP only provides its protections over the part of the datagram that ESP encapsulates. The authentication services of ESP are optional. These services enable you to use ESP and AH together on the same datagram without redundancy. Because ESP uses encryption-enabling technology, ESP must conform to U.S. export control laws.

ESP encapsulates its data, so ESP only protects the data that follows its beginning in the datagram, as shown in the following illustration.



■ Encrypted

In a TCP packet, ESP encapsulates only the TCP header and its data. If the packet is an IP-in-IP datagram, ESP protects the inner IP datagram. Per-socket policy allows *self-encapsulation*, so ESP can encapsulate IP options when ESP needs to. For further discussion, see “[Transport and Tunnel Modes in IPsec](#)” on page 435.

Security Considerations When Using AH and ESP

The following table compares the protections that are provided by AH and ESP.

TABLE 18–2 Protections Provided by AH and ESP in IPsec

Protocol	Packet Coverage	Protection	Against Attacks
AH	Protects packet from the IP header to the transport header	Provides strong integrity, data authentication: <ul style="list-style-type: none"> ■ Ensures that the receiver receives exactly what the sender sent ■ Is susceptible to replay attacks when an AH does not enable replay protection 	Replay, cut-and-paste
ESP	Protects packet following the beginning of ESP in the datagram.	With encryption option, encrypts the IP datagram. Ensures confidentiality With authentication option, provides the same protection as AH With both options, provides strong integrity, data authentication, and confidentiality	Eavesdropping Replay, cut-and-paste Replay, cut-and-paste, eavesdropping

Authentication and Encryption Algorithms in IPsec

IPsec security protocols use two types of algorithms, authentication and encryption. The AH module uses authentication algorithms. The ESP module can use encryption as well as authentication algorithms. You can obtain a list of the algorithms on your system and their properties by using the `ipsecalgs` command. For more information, see the `ipsecalgs(1M)` man page. You can also use the functions that are described in the `getipsecalgbyname(3NSL)` man page to retrieve the properties of algorithms.

IPsec on a Solaris system uses the Solaris cryptographic framework to access the algorithms. The framework provides a central repository for algorithms, in addition to other services. The framework enables IPsec to take advantage of high performance

cryptographic hardware accelerators. The framework also provides resource control features. For example, the framework enables you to limit the amount of CPU time spent in cryptographic operations in the kernel. For more information, see the following:

- Chapter 13, “Solaris Cryptographic Framework (Overview),” in *System Administration Guide: Security Services*
- Chapter 8, “Introduction to the Solaris Cryptographic Framework,” in *Solaris Security for Developers Guide*

Authentication Algorithms in IPsec

Authentication algorithms produce an integrity checksum value or *digest* that is based on the data and a key. The AH module uses authentication algorithms. The ESP module can use authentication algorithms as well.

Encryption Algorithms in IPsec

Encryption algorithms encrypt data with a key. The ESP module in IPsec uses encryption algorithms. The algorithms operate on data in units of a *block size*. By default, the DES-CBC, 3DES-CBC, AES-CBC, and Blowfish-CBC algorithms are installed. The key sizes that are supported by the AES-CBC and Blowfish-CBC algorithms are limited to 128 bits.

AES-CBC and Blowfish-CBC algorithms that support key sizes that are greater than 128 bits are available to IPsec when you install the Solaris Encryption Kit. Because of export laws in the United States, not all encryption algorithms are available outside of the United States. The kit is available on a separate CD that is *not* part of the Solaris 10 installation box. The *Solaris 10 Encryption Kit Installation Guide* describes how to install the kit. For more information, see the <http://www.sun.com/security/encryption> web site.

IPsec Protection Policies

IPsec protection policies can use any of the security mechanisms. IPsec policies can be applied at the following levels:

- On a system-wide level
- On a per-socket level

IPsec applies the system-wide policy to outbound datagrams and inbound datagrams. Outbound datagrams are either sent with protection or without protection. If protection is applied, the algorithms are either specific or non-specific. You can apply some additional rules to outbound datagrams, because of the additional data that is

known by the system. Inbound datagrams can be either accepted or dropped. The decision to drop or accept an inbound datagram is based on several criteria, which sometimes overlap or conflict. Conflicts are resolved by determining which rule is parsed first. The traffic is automatically accepted, except when a policy entry states that traffic should bypass all other policies.

The policy that normally protects a datagram can be bypassed. You can either specify an exception in the system-wide policy, or you can request a bypass in the per-socket policy. For traffic within a system, policies are enforced, but actual security mechanisms are not applied. Instead, the outbound policy on an intra-system packet translates into an inbound packet that has had those mechanisms applied.

You use the `ipsecinit.conf` file and the `ipsecconf` command to configure IPsec policies. For details and examples, see the `ipsecconf(1M)` man page.

Transport and Tunnel Modes in IPsec

The Solaris implementation of IPsec is primarily an implementation of IPsec in transport mode. When you invoke ESP or AH after the IP header to protect a datagram, you are using transport mode. An example follows. A packet begins with the following header:

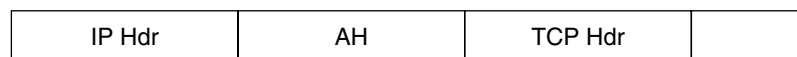


ESP, in transport mode, protects the data as follows:



■ Encrypted

AH, in transport mode, protects the data as follows:



AH actually covers the data before the data appears in the datagram. Consequently, the protection that is provided by AH, even in transport mode, covers some of the IP header.

Tunnel mode is implemented as a special instance of the transport mode. The implementation treats IP-in-IP tunnels as a special transport provider. When an entire datagram is *inside* the protection of an IPsec header, IPsec is protecting the datagram in tunnel mode. Because AH covers most of its preceding IP header, tunnel mode is usually performed only on ESP. The preceding example datagram would be protected in tunnel mode as follows:



■ Encrypted

In tunnel mode, the inner header is protected, while the outer IP header is unprotected. Often, the outer IP header has different source and different destination addresses from the inner IP header. The inner and outer IP headers can match if, for example, an IPsec-aware network program uses self-encapsulation with ESP. Self-encapsulation with ESP protects an IP header option.

The `ifconfig` configuration options to set tunnels are nearly identical to the options that are available to socket programmers when enabling per-socket IPsec. Also, tunnel mode can be enabled in per-socket IPsec. In per-socket tunnel mode, the inner packet IP header has the same addresses as the outer IP header.

- For details on per-socket policy, see the `ipsec(7P)` man page.
- For an example of per-socket policy, see [“How to Secure a Web Server With IPsec” on page 447](#).
- For more information about tunnels, see the `ifconfig(1M)` man page.
- For an example of tunnel configuration, see [“How to Set Up a VPN With IPsec Over IPv4” on page 450](#).

Virtual Private Networks and IPsec

A configured tunnel is a point-to-point interface. The tunnel enables one IP packet to be encapsulated within another IP packet. A correctly configured tunnel requires both a tunnel source and a tunnel destination. For more information, see the `tun(7M)` man page and [“Configuring Tunnels for IPv6 Support” on page 130](#).

A tunnel creates an apparent [physical interface](#) to IP. The physical link’s integrity depends on the underlying security protocols. If you set up the security associations (SAs) securely, then you can trust the tunnel. Packets that exit the tunnel must have originated from the peer that was specified in the tunnel destination. If this trust exists, you can use per-interface IP forwarding to create a [virtual private network \(VPN\)](#).

You can use IPsec to construct a VPN. IPsec secures the connection. For example, an organization that uses VPN technology to connect offices with separate networks can deploy IPsec to secure traffic between the two offices.

The following figure illustrates how two offices use the Internet to form their VPN with IPsec deployed on their network systems.

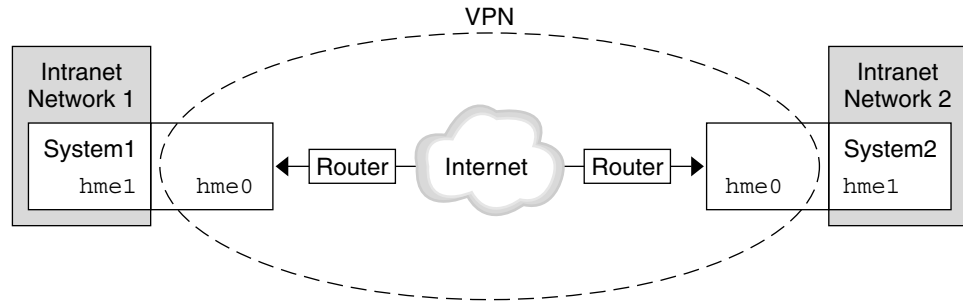


FIGURE 18-3 Virtual Private Network

For a detailed example of the setup procedure, see [“How to Set Up a VPN With IPsec Over IPv4”](#) on page 450. For IPv6 networks, see [“How to Set Up a VPN With IPsec Over IPv6”](#) on page 456.

IPsec and NAT Traversal

IKE can negotiate IPsec SAs across a NAT box. This ability enables systems to securely connect from a remote network, even when the systems are behind a NAT device. For example, employees who work from home, or who log on from a conference site can protect their traffic with IPsec.

NAT stands for network address translation. A NAT box is used to translate a private internal address into a unique Internet address. NATs are very common at public access points to the Internet, such as hotels. For a fuller discussion, see [“Using Solaris IP Filter’s NAT Feature”](#) on page 540.

The ability to use IKE when a NAT box is between communicating systems is called NAT traversal, or NAT-T. In the Solaris 10 release, NAT-T has the following limitations:

- NAT-T works on IPv4 networks only.
- NAT-T cannot take advantage of the IPsec ESP acceleration provided by the Sun Crypto Accelerator 4000 board. However, IKE acceleration with the Sun Crypto Accelerator 4000 board works.

- The AH protocol depends on an unchanging IP header, therefore AH cannot work with NAT-T. The ESP protocol is used with NAT-T.
- The NAT box does not use special processing rules. A NAT box with special IPsec processing rules might interfere with the implementation of NAT-T.
- NAT-T works only when the IKE initiator is the system behind the NAT box. An IKE responder cannot be behind a NAT box unless the box has been programmed to forward IKE packets to the appropriate individual system behind the box.

The following RFCs and drafts describe NAT functionality and the limits of NAT-T. Copies of the RFCs can be retrieved from <http://www.rfc-editor.org>. Copies of the drafts can be retrieved from <http://www.ietf.org/1id-abstracts.html>.

- RFC 3022, "Traditional IP Network Address Translator (Traditional NAT)," January 2001
- RFC 3715, "IPsec-Network Address Translation (NAT) Compatibility Requirements," March 2004
- Draft, "UDP Encapsulation of IPsec Packets," `draft-ietf-ipsec-udp-encaps-09.txt`, May 2004
- Draft, "Negotiation of NAT-Traversal in the IKE," `draft-ietf-ipsec-nat-t-ike-08.txt`, February 2004

To use IPsec across a NAT, see ["Configuring IKE for Mobile Systems \(Task Map\)" on page 512](#).

IPsec and SCTP

The Solaris 10 release supports the Streams Control Transmission Protocol (SCTP). The use of the SCTP protocol and SCTP port number to specify IPsec policy is supported, but is not robust. The IPsec extensions for SCTP as specified in RFC 3554 are not yet implemented. These limitations can create complications in creating IPsec policy for SCTP.

SCTP can make use of multiple source and destination addresses in the context of a single SCTP association. When IPsec policy is applied to a single source or a single destination address, communication can fail when SCTP switches the source or the destination address of that association. IPsec policy only recognizes the original address. For information about SCTP, read the RFCs and ["SCTP Protocol" on page 40](#).

IPsec and Solaris Zones

IPsec can be configured from the global zone. IPsec policy can be applied to the global zone, or to a non-global zone. For information on how to use IPsec with zones, see [“Configuring IPsec” on page 444](#). For information about zones, see Chapter 16, *“Introduction to Solaris Zones,”* in *System Administration Guide: Solaris Containers—Resource Management and Solaris Zones*.

IPsec Utilities and Files

[Table 18–3](#) describes the files and commands that are used to configure and manage IPsec. For completeness, the table includes key management files and commands.

- For instructions on implementing IPsec on your network, see [“Configuring IPsec \(Task Map\)” on page 443](#).
- For more details about IPsec utilities and files, see [Chapter 20](#).

TABLE 18–3 List of Selected IPsec Files and Commands

IPsec Utility or File	Description	Man Page
<code>/etc/inet/ipsecinit.conf</code> file	IPsec policy file. If this file exists, IPsec is activated at boot time.	<code>ipseconf(1M)</code>
<code>ipsecpolicy.conf</code> file	Temporary IPsec policy file. Created when the <code>ipseconf</code> command updates IPsec policy.	
<code>ipseconf</code> command	IPsec policy command. The boot scripts use <code>ipseconf</code> to read the <code>/etc/inet/ipsecinit.conf</code> file and activate IPsec. Useful for viewing and modifying the current IPsec policy, and for testing.	<code>ipseconf(1M)</code>
<code>PF_KEY</code> socket interface	Interface for security associations database (SADB). Handles manual key management and automatic key management.	<code>pf_key(7P)</code>
<code>ipseckey</code> command	IPsec security associations (SAs) keying command. <code>ipseckey</code> is a command-line front end to the <code>PF_KEY</code> interface. <code>ipseckey</code> can create, destroy, or modify SAs.	<code>ipseckey(1M)</code>
<code>/etc/inet/secret/ipseckeys</code> file	Keys for IPsec SAs. If the <code>ipsecinit.conf</code> file exists, the <code>ipseckeys</code> file is automatically read at boot time.	

TABLE 18-3 List of Selected IPsec Files and Commands (Continued)

IPsec Utility or File	Description	Man Page
<code>ipsecalgs</code> command	IPsec algorithms command. Useful for viewing and modifying the list of IPsec algorithms and their properties.	<code>ipsecalgs(1M)</code>
<code>/etc/inet/ipsecalgs</code> file	Contains the configured IPsec protocols and algorithm definitions. This file is managed by the <code>ipsecalgs</code> utility and must never be edited manually.	
<code>/etc/inet/ike/config</code> file	IKE configuration and policy file. If this file exists, the IKE daemon, <code>in.iked</code> , provides automatic key management. The management is based on rules and global parameters in the <code>/etc/inet/ike/config</code> file. See “IKE Utilities and Files” on page 482.	<code>ike.config(4)</code>

Changes to IPsec for the Solaris 10 Release

Since the Solaris 9 release, IPsec includes the following functionality:

- When a Sun Crypto Accelerator 4000 board is attached, the board automatically caches IPsec SAs for packets that use the board’s Ethernet interface. The board also accelerates the processing of the IPsec SAs.
- IPsec can take advantage of automatic key management with IKE over IPv6 networks. For more information, see [Chapter 21](#).
For new IKE features, see “[Changes to IKE for the Solaris 10 Release](#)” on page 483.
- The parser for the `ipseckey` command provides clearer help. The `ipseckey monitor` command timestamps each event. For details, see the `ipseckey(1M)` man page.
- IPsec algorithms now come from a central storage location, the Solaris cryptographic framework. The `ipsecalgs(1M)` man page describes the characteristics of the algorithms that are available. The algorithms are optimized for the architecture that they run on. For a description of the framework, see [Chapter 13, “Solaris Cryptographic Framework \(Overview\),”](#) in *System Administration Guide: Security Services*.
- IPsec works in the global zone. IPsec policy is managed in the global zone for a non-global zone. Keying material is created and is managed manually in the global zone for a non-global zone. IKE cannot be used to generate keys for a non-global zone. For more information on zones, see [Chapter 16, “Introduction to Solaris Zones,”](#) in *System Administration Guide: Solaris Containers—Resource Management and Solaris Zones*.

- IPsec policy can work with the Streams Control Transmission Protocol (SCTP) and SCTP port number. However, the implementation is not complete. The IPsec extensions for SCTP that are specified in RFC 3554 are not yet implemented. These limitations can cause complications when creating IPsec policy for SCTP. For details, consult the RFCs. Also, read [“IPsec and SCTP” on page 438](#) and [“SCTP Protocol” on page 40](#).
- IPsec and IKE can protect traffic that originates behind a NAT box. For details and limitations, see [“IPsec and NAT Traversal” on page 437](#). For procedures, see [“Configuring IKE for Mobile Systems \(Task Map\)” on page 512](#).

Configuring IPsec (Tasks)

This chapter provides procedures for implementing IPsec on your network. The procedures are described in “[Configuring IPsec \(Task Map\)](#)” on page 443.

For overview information about IPsec, see [Chapter 18](#). For reference information about IPsec, see [Chapter 20](#).

Configuring IPsec (Task Map)

The following table points to procedures that set up IPsec between one or more systems. The `ipseccnf(1M)`, `ipseckey(1M)`, and `ifconfig(1M)` man pages also describe useful procedures in their respective Examples sections.

Task	Description	For Instructions
Secure traffic between two systems	Protects packets from one system to another system.	“ How to Secure Traffic Between Two Systems With IPsec ” on page 445
Secure a web server by using IPsec policy	Requires non-web traffic to use IPsec. Web clients are identified by particular ports, which bypass IPsec checks.	“ How to Secure a Web Server With IPsec ” on page 447
Display IPsec policies	Displays the IPsec policies that are currently being enforced, and the order in which the policies are enforced.	“ How to Display IPsec Policies ” on page 449
Set up a virtual private network (VPN)	Sets up IPsec between two systems that are separated by the Internet.	“ How to Set Up a VPN With IPsec Over IPv4 ” on page 450
		“ How to Set Up a VPN With IPsec Over IPv6 ” on page 456

Task	Description	For Instructions
Generate random numbers	Generates random numbers for keying material for manually created security associations.	“How to Generate Random Numbers on a Solaris System” on page 460
Create or replace security associations manually	Provides the raw data for security associations: <ul style="list-style-type: none"> ■ IPsec algorithm name and keying material ■ Key for the security parameter index ■ IP source and destination addresses 	“How to Manually Create IPsec Security Associations” on page 461
Check that IPsec is protecting the packets	Examines snoop output for specific headers that indicate how the IP datagrams are protected.	“How to Verify That Packets Are Protected With IPsec” on page 465
(Optional) Create a Network Security role	Creates a role that can set up a secure network, but has fewer powers than superuser.	“How to Create a Role for Configuring Network Security” on page 467

Configuring IPsec

This section provides procedures that enable you to secure traffic between two systems, to secure a web server, and to set up a virtual private network (VPN). Additional procedures provide keying material, provide security associations, and verify that IPsec is working as configured.

The following information applies to all IPsec configuration tasks:

- **IPsec and zones** – To manage IPsec policy and keys for a non-global zone, run the `ipseckey` and `ipseccnf` commands from the global zone. Use the source address which corresponds to the non-global zone that is being configured. You can also configure IPsec policy and keys in the global zone for the global zone. You cannot use IKE to manage keys in a non-global zone.
- **IPsec and RBAC** – To use roles to administer IPsec, see Chapter 9, “Using Role-Based Access Control (Tasks),” in *System Administration Guide: Security Services*.
- **IPsec and SCTP** – IPsec can be used to protect Streams Control Transmission Protocol (SCTP) associations, but caution must be used. For more information, see [“IPsec and SCTP” on page 438](#).

▼ How to Secure Traffic Between Two Systems With IPsec

Note – You configure IPsec policy for a non-global zone in the global zone. If you are configuring IPsec for a non-global zone, you must manually create keys (SAs) with the `ipseckey` command. You cannot use IKE.

This procedure assumes the following setup:

- The two systems are named `enigma` and `partym`.
- Each system has two addresses, an IPv4 address and an IPv6 address.
- Each system invokes AH protection with the MD5 algorithm, which requires a key of 128 bits.
- Each system invokes ESP protections with the 3DES algorithm, which requires a key of 192 bits.
- Each system uses shared security associations.

With shared SAs, only one pair of SAs is needed to protect the two systems.

Steps 1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **On each system, add host entries.**

Add the addresses and host name for the other system in the `/etc/inet/ipnodes` file. The entries for one system must be contiguous in the file. For more information on system configuration files, see “TCP/IP Configuration Files” on page 183 and Chapter 10.

If you are connecting systems with IPv4 addresses only, you modify the `/etc/inet/hosts` file.

a. **On a system that is named `partym`, type the following in the `ipnodes` file:**

```
# Secure communication with enigma
192.168.116.16 enigma
```

```
2001::aaaa:6666:6666 enigma
```

- b. On a system that is named enigma, type the following in the ipnodes file:**

```
# Secure communication with partym
192.168.13.213 partym
2001::eeee:3333:3333 partym
```

This step enables the boot scripts to use the system names without depending on nonexistent naming services.

- 3. On each system, create the file /etc/inet/ipsecinit.conf.**

For an example, see the /etc/inet/ipsecinit.sample file.

- 4. Add an IPsec policy entry to the ipsecinit.conf file.**

- a. On the enigma system, add the following policy to the ipsecinit.conf file:**

```
{laddr enigma raddr partym} ipsec {auth_algs any encr_algs any sa shared}
```

- b. On the partym system, add the same policy to its ipsecinit.conf file:**

```
{laddr partym raddr enigma} ipsec {auth_algs any encr_algs any sa shared}
```

For the syntax of IPsec policy entries, see the ipsecconf(1M) man page.

- 5. On each system, add a pair of IPsec SAs between the two systems.**

You can configure Internet Key Exchange (IKE) to create the SAs automatically. You can also add the SAs manually.

Note – You should use IKE unless you have good reason to generate and maintain your keys manually. IKE key management is more secure than manual key management.

- Configure IKE by following one of the configuration procedures in “[Configuring IKE \(Task Map\)](#)” on page 485. For the syntax of the IKE configuration file, see the `ike.config(4)` man page.
- If you are going to add the SAs manually, see “[How to Manually Create IPsec Security Associations](#)” on page 461.

- 6. Reboot each system.**

```
# init 6
```

- 7. Verify that packets are being protected.**

For the procedure, see “[How to Verify That Packets Are Protected With IPsec](#)” on page 465.

Example 19–1 Securing Traffic With IPsec Without Rebooting

The following example describes how to implement IPsec in a test environment. In a production environment, it is more secure to reboot than to run the `ipseccnf` command.

Instead of rebooting at Step 6 of “How to Secure Traffic Between Two Systems With IPsec” on page 445, choose one of the following options.

- If you used IKE to create keying material, stop and then restart the `in.iked` daemon.

```
# pkill in.iked
# /usr/lib/inet/in.iked
```

- If you added keys manually, use the `ipseckey` command to add the SAs to the database. Then activate the IPsec policy with the `ipseccnf` command.

```
# ipseckey -f /etc/inet/secret/ipseckey
# ipseccnf -a /etc/inet/ipsecinit.conf
```

Security Considerations – Read the warning when you execute the `ipseccnf` command. A socket that is already latched, that is, a socket that is already in use, provides an unsecured back door into the system. For more extensive discussion, see “Security Considerations for `ipsecinit.conf` and `ipseccnf`” on page 471.

▼ How to Secure a Web Server With IPsec

A secure web server allows web clients to talk to the web service. On a secure web server, traffic that is not web traffic *must* pass security checks. The following procedure includes bypasses for web traffic. In addition, this web server can make nonsecured DNS client requests. All other traffic requires ESP with Blowfish and SHA algorithms.

Note – You configure IPsec policy for a non-global zone in the global zone. If you are configuring IPsec for a non-global zone, you must manually create keys (SAs) with the `ipseckey` command. You cannot use IKE.

- Steps**
1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. Determine which services need to bypass security policy checks.

For a web server, these services include TCP ports 80 (HTTP) and 443 (Secure HTTP). If the web server provides DNS name lookups, the server might also need to include port 53 for both TCP and UDP.

3. Create a file in the `/etc/inet` directory for the web server policy.

Give the file a name that indicates its purpose, for example `IPsecWebInitFile`. Type the following lines in this file:

```
# Web traffic that web server should bypass.
{lport 80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with Blowfish and SHA-1.
# Use a unique SA for outbound traffic from the port
{} permit {encr_algs blowfish encr_auth_algs sha}
{} apply {encr_algs blowfish encr_auth_algs sha sa}
```

This configuration allows only secure traffic to access the system, with the bypass exceptions that are described in [Step 2](#).

4. Copy the contents of the file that you created in [Step 3](#) into the `/etc/inet/ipsecinit.conf` file.

5. Protect the `IPsecWebInitFile` file with read-only permissions.

```
# chmod 400 IPsecWebInitFile
```

6. Secure the web server without rebooting.

Choose one of the following options.

- If you are using IKE for key management, stop and restart the `in.iked` daemon.

```
# pkill in.iked
# /usr/lib/inet/in.iked
```

- If you are manually managing keys, use the `ipseckey` and `ipseccnf` commands.

Use the `IPsecWebInitFile` as the argument to the `ipseccnf` command. If you use the `ipsecinit.conf` file as the argument, the `ipseccnf` command generates errors when policies in the file are already implemented on the system.


```
# ipseckey -f /etc/inet/secret/ipseckey  
# ipsecconf -a /etc/inet/IPsecWebInitFile
```



Caution – Read the warning when you execute the `ipsecconf` command. A socket that is already latched, that is, a socket that is already in use, provides an unsecured back door into the system. For more extensive discussion, see “[Security Considerations for `ipsecinit.conf` and `ipsecconf`](#)” on page 471. The same warning applies to restarting the `in.iked` daemon.

You can also reboot. Rebooting ensures that the IPsec policy is in effect on all TCP connections. At reboot, the TCP connections use the policy in the IPsec policy file.

7. **(Optional) Enable a remote system to communicate with the web server for nonweb traffic.**

Type the following policy in a remote system’s `ipsecinit.conf` file.

```
# Communicate with web server about nonweb stuff  
#  
{saddr webserver} permit {encr_algs blowfish encr_auth_algs sha}  
{saddr webserver} apply {encr_algs blowfish encr_auth_algs sha sa shared}
```

A remote system can communicate securely with the web server for nonweb traffic only when the systems’ IPsec policies match.

▼ How to Display IPsec Policies

You can see the policies that are configured in the system when you issue the `ipsecconf` command without any arguments. The command must be run from the global zone.

- Steps**
1. **Assume a role that includes the Network Security profile, or become superuser.**
To create a role that includes the Network Security profile and assign that role to a user, see “[How to Create a Role for Configuring Network Security](#)” on page 467.

2. **Display the IPsec policy entries in the order that the entries were added.**

```
$ ipsecconf
```

The command displays each entry with an *index* followed by a number.

3. **Display the IPsec policy entries in the order in which the traffic match occurs.**

```
$ ipsecconf -l
```

▼ How to Set Up a VPN With IPsec Over IPv4

This procedure shows you how to set up a virtual private network (VPN) by using the Internet to connect two networks within an organization. The procedure then shows you how to secure the traffic between the networks with IPsec.

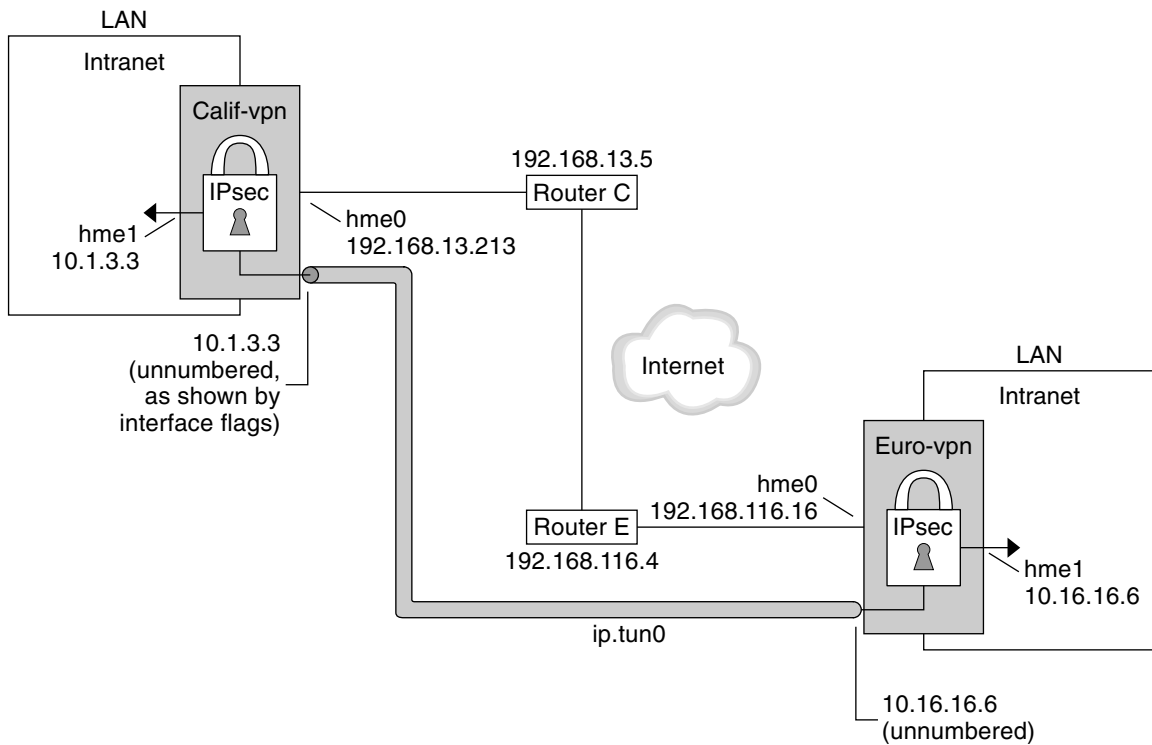
This procedure extends the procedure, [“How to Secure Traffic Between Two Systems With IPsec” on page 445](#). In addition to connecting two systems, you are connecting two intranets that connect to these two systems. The systems in this procedure function as gateways.

Note – You configure IPsec policy for a non-global zone in the global zone. If you are configuring IPsec for a non-global zone, you must manually create keys (SAs) with the `ipseckey` command. You cannot use IKE.

This procedure assumes the following setup:

- Each system is using an IPv4 address space.
For a similar example with IPv6 addresses, see [“How to Set Up a VPN With IPsec Over IPv6” on page 456](#).
- Each system has two interfaces. The `hme0` interface connects to the Internet. In this example, Internet IP addresses begin with 192.168. The `hme1` interface connects to the company’s local area network (LAN), its intranet. In this example, intranet IP addresses begin with the number 10.
- Each system invokes AH protection with the MD5 algorithm. The MD5 algorithm requires a 128-bit key.
- Each system invokes ESP protection with the 3DES algorithm. The 3DES algorithm requires a 192-bit key.
- Each system can connect to a router that has direct access to the Internet.
- Each system uses shared security associations.

For a description of VPNs, see [“Virtual Private Networks and IPsec” on page 436](#). The following figure describes the VPN that this procedure configures.



hme0 = Turn off IP forwarding

hme1 = Turn on IP forwarding

ip.tun = Turn on IP forwarding

Router C — /etc/defaultrouter for Calif-vpn

Router E — /etc/defaultrouter for Euro-vpn

This procedure uses the following configuration parameters.

Parameter	Europe	California
System name	enigma	partym
System intranet interface	hme1	hme1
System Internet interface	hme0	hme0
System intranet address, also the <i>-point</i> address in Step 7	10.16.16.6	10.1.3.3

Parameter	Europe	California
System Internet address, also the <i>-taddr</i> address in Step 7	192.168.116.16	192.168.13.213
Name of Internet router	router-E	router-C
Address of Internet router	192.168.116.4	192.168.13.5
Tunnel name	ip.tun0	ip.tun0

Steps 1. **On the system console on one of the systems, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Ensure that IP forwarding and IP dynamic routing are disabled.**

```
# routeadm
Configuration      Current      Current
      Option      Configuration System State
-----
IPv4 forwarding    disabled     disabled
  IPv4 routing     default (enabled) enabled
...
```

If forwarding and routing are enabled, you can disable them by typing:

```
# routeadm -d ipv4-routing -d ipv4-forwarding
# routeadm -u
```

Turning off IP forwarding prevents packets from being forwarded from one network to another network through this system. For a description of the `routeadm` command, see the `routeadm(1M)` man page.

3. **Turn on IP strict destination multihoming.**

```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```

Turning on IP strict destination multihoming ensures that packets for one of the system’s destination addresses arrive at the correct destination address.

When you turn off IP forwarding and turn on IP strict destination multihoming, fewer packets flow all the way through the system. When strict destination multihoming is enabled, packets that arrive on a particular interface must be addressed to one of the local IP addresses of that interface. All other packets, even ones that are addressed to other local addresses of the system, are dropped.

4. Disable most network services, and possibly all network services.

The disabling of network services prevents IP packets from doing any harm to the system. For example, an SNMP daemon, a telnet connection, or an rlogin connection could be exploited.

Note – The VPN router should allow very few incoming requests. You need to disable all processes that accept incoming traffic.

For example, the following commands disable many network services, while leaving some network services, such as Solaris Secure Shell, enabled:

```
# svcadm disable network/ftp:default
# svcadm disable network/finger:default
# svcadm disable network/login:rlogin
# svcadm disable network/nfs/server:default
# svcadm disable network/rpc/rstat:default
# svcadm disable network/smtp:sendmail
# svcadm disable network/telnet:default
# svcs | grep network
online      Aug_02    svc:/network/loopback:default
...
online      Aug_09    svc:/network/ssh:default
...
```

5. On each system, add a pair of SAs between the two systems.

Choose one of the following options:

- Configure IKE to manage the keys for the SAs. Use one of the procedures in “Configuring IKE (Task Map)” on page 485 to configure IKE for the VPN.
- If you have an overriding reason to manually manage the keys, see “How to Manually Create IPsec Security Associations” on page 461.

6. On each system, add IPsec policy.

Edit the `/etc/inet/ipsecinit.conf` file to add the IPsec policy for the VPN. To strengthen the policy, see [Example 19–2](#).

a. For example, on the `enigma` system, type the following entry into the `ipsecinit.conf` file:

```
# LAN traffic can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with 3DES and MD5.
{} ipsec {encr_algs 3des encr_auth_algs md5}
```

b. On the `partym` system, type the following entry into the `ipsecinit.conf` file:

```
# LAN traffic can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}
```

```
# WAN traffic uses ESP with 3DES and MD5.
{} ipsec {encr_algs 3des encr_auth_algs md5}
```

7. On each system, configure a secure tunnel, ip.tun0.

The tunnel adds another physical interface from the IP perspective. Type the following three `ifconfig` commands to create the point-to-point interface:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 system1-point system2-point \
tsrc system1-taddr tdst system2-taddr \
encr_algs 3des encr_auth_algs md5

# ifconfig ip.tun0 router up
```

a. For example, on the enigma system, type the following commands:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.16.16.6 10.1.3.3 \
tsrc 192.168.116.16 tdst 192.168.13.213 \
encr_algs 3des encr_auth_algs md5

# ifconfig ip.tun0 router up
```

b. On the partym system, type the following commands:

```
# ifconfig ip.tun0 plumb

# ifconfig ip.tun0 10.1.3.3 10.16.16.6 \
tsrc 192.168.13.213 tdst 192.168.116.16 \
encr_algs 3des encr_auth_algs md5

# ifconfig ip.tun0 router up
```

The IPsec policy that is passed to the `ifconfig` commands must be the same as the IPsec policy in the `ipsecinit.conf` file. Upon reboot, each system reads the `ipsecinit.conf` file for its policy.

8. On each system, turn on IP forwarding for the hme1 interface.

```
# ifconfig hme1 router
```

IP forwarding means that packets that arrive from somewhere else can be forwarded. IP forwarding also means that packets that leave this interface might have originated somewhere else. To successfully forward a packet, both the receiving interface and the transmitting interface must have IP forwarding turned on.

Because the `hme1` interface is *inside* the intranet, IP forwarding must be turned on for `hme1`. Because `ip.tun0` connects the two systems through the Internet, IP forwarding must be turned on for `ip.tun0`.

The `hme0` interface has its IP forwarding turned off to prevent an *outside* adversary from injecting packets into the protected intranet. The *outside* refers to the Internet.

9. On each system, ensure that routing protocols do not advertise the default route within the intranet.

```
# ifconfig hme0 private
```

Even if `hme0` has IP forwarding turned off, a routing protocol implementation might still advertise the interface. For example, the `in.routed` protocol might still advertise that `hme0` is available to forward packets to its peers inside the intranet. By setting the interface's *private* flag, these advertisements are prevented.

10. Manually, add a default route over `hme0`.

The default route should be a router with direct access to the Internet.

```
# route add default router-on-hme0-subnet
```

- a. For example, on the `enigma` system, add the following route:

```
# route add default 192.168.116.4
```

- b. On the `partym` system, add the following route:

```
# route add default 192.168.13.5
```

Even though the `hme0` interface is not part of the intranet, `hme0` does need to reach across the Internet to its peer system. To find its peer, `hme0` needs information about Internet routing. The VPN system appears to be a host, rather than a router, to the rest of the Internet. Therefore, you can use a default router or run the router discovery protocol to find a peer system. For more information, see the `route(1M)` and `in.routed(1M)` man pages.

11. Ensure that the VPN starts after a reboot by adding an entry to the `/etc/hostname.ip.tun0` file.

```
system1-point system2-point tsrc system1-taddr \  
tdst system2-taddr encr_algs 3des encr_auth_algs md5 router up
```

- a. For example, on the `enigma` system, add the following entry to the `hostname.ip.tun0` file:

```
10.16.16.6 10.1.3.3 tsrc 192.168.116.16 \  
tdst 192.168.13.213 encr_algs 3des encr_auth_algs md5 router up
```

- b. On the `partym` system, add the following entry to the `hostname.ip.tun0` file:

```
10.1.3.3 10.16.16.6 tsrc 192.168.13.213 \  
tdst 192.168.116.16 encr_algs 3des encr_auth_algs md5 router up
```

12. On each system, configure the interface files to pass the correct parameters to the routing daemon.

- a. On the enigma system, modify the `/etc/hostname.interface` files.

```
# cat enigma hostname.hme0
10.16.16.6 private

# cat enigma hostname.hme1
192.168.116.16 router
```

- b. On the partym system, modify the `/etc/hostname.interface` files.

```
# cat partym hostname.hme0
10.1.3.3 private

# cat partym hostname.hme1
192.168.13.213 router
```

13. On each system, run a routing protocol.

You might need to configure the routing protocol before enabling routing. For more information, see [“Routing Protocols in the Solaris OS”](#) on page 201. For a procedure, see [“How to Configure an IPv4 Router”](#) on page 119.

```
# routeadm -e ipv4-routing
# routeadm -u
```

Example 19–2 Requiring IPsec Policy on All Systems on a LAN

In this example, the LAN policy does not bypass IPsec. The IPsec policy that was set in [Step 6](#) is strengthened. With this policy configuration, each system on the LAN must activate IPsec to communicate with the router.

```
# LAN traffic must implement IPsec.
# {laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with 3DES and MD5.
{} ipsec {encr_algs 3des encr_auth_algs md5}
```

▼ How to Set Up a VPN With IPsec Over IPv6

To set up a VPN on an IPv6 network, you follow the same steps as for an IPv4 network. However, the syntax of the commands is slightly different. For a fuller description of the reasons for running particular commands, see [“How to Set Up a VPN With IPsec Over IPv4”](#) on page 450. The IPv4 procedure also includes a picture of the VPN.

This procedure uses the following configuration parameters.

Parameter	Europe	California
System name	enigma	partym
System intranet interface	hme1	hme1
System Internet interface	hme0	hme0
System intranet address	6000:6666::aaaa:1116	6000:3333::eeee:1113
System Internet address	2001::aaaa:6666:6666	2001::eeee:3333:3333
Name of Internet router	router-E	router-C
Address of Internet router	2001::aaaa:0:4	2001::eeee:0:1
Tunnel name	ip6.tun0	ip6.tun0

- Steps** 1. **On the system console on one of the systems, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Ensure that IP forwarding and IP dynamic routing are disabled.**

```
# routeadm
Configuration      Current      Current
      Option      Configuration System State
-----
...
IPv6 forwarding    disabled     disabled
      IPv6 routing disabled     disabled
```

If forwarding and routing are enabled, you can disable them by typing:

```
# routeadm -d ipv6-forwarding -d ipv6-routing
# routeadm -u
```

3. **Turn on IP strict destination multihoming.**

```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```

4. **Disable most network services, and possibly all network services.**

For example, the following commands disable remote logins, while leaving some network services, such as Solaris Secure Shell, enabled:

```
# svcadm disable network/ftp:default
# svcadm disable network/login:rlogin
# svcadm disable network/telnet:default
# svcs | grep network
online      Aug_02   svc:/network/loopback:default
...
online      Aug_09   svc:/network/ssh:default
...
```

5. On each system, add a pair of SAs between the two systems.

Choose one of the following options.

- Configure IKE to manage the keys for the SAs. Use one of the procedures in “Configuring IKE (Task Map)” on page 485 to configure IKE for the VPN.
- If you have an overriding reason to manually manage the keys, see “How to Manually Create IPsec Security Associations” on page 461.

6. On each system, add IPsec policy.

Edit the `/etc/inet/ipsecinit.conf` file to add the IPsec policy for the VPN.

a. For example, on the `enigma` system, type the following entry into the `ipsecinit.conf` file:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:6666::aaaa:1116 dir both} bypass {}

# WAN traffic uses ESP with 3DES and MD5.
{} ipsec {encr_algs 3des encr_auth_algs md5}
```

b. On the `partym` system, type the following entry into the `ipsecinit.conf` file:

```
# IPv6 Neighbor Discovery messages bypass IPsec.
{ulp ipv6-icmp type 133-137 dir both} pass {}

# LAN traffic can bypass IPsec.
{laddr 6000:3333::eeee:1113 dir both} bypass {}

# WAN traffic uses ESP with 3DES and MD5.
{} ipsec {encr_algs 3des encr_auth_algs md5}
```

7. On each system, configure a secure tunnel, `ip6.tun0`.

a. For example, on the `enigma` system, type the following commands:

```
# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:6666::aaaa:1116 6000:3333::eeee:1113 \
```

```

tsrc 2001::aaaa:6666:6666 \
tdst 2001::eeee:3333:3333 \
encr_algs 3des encr_auth_algs md5

# ifconfig ip6.tun0 inet6 router up

```

- b. On the `partym` system, type the following commands:

```

# ifconfig ip6.tun0 inet6 plumb

# ifconfig ip6.tun0 inet6 6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333 \
tdst 2001::aaaa:6666:6666 \
encr_algs 3des encr_auth_algs md5

# ifconfig ip6.tun0 inet6 router up

```

8. On each system, turn on IP forwarding for the `hme1` interface.

```
# ifconfig hme1 router
```

9. On each system, ensure that routing protocols do not advertise the default route within the intranet.

```
# ifconfig hme0 private
```

10. Manually, add a default route over `hme0`.

- a. For example, on the `enigma` system, add the following route:

```
# route add -inet6 default 2001::aaaa:0:4
```

- b. On the `partym` system, add the following route:

```
# route add -inet6 default 2001::eeee:0:1
```

11. Ensure that the VPN starts after a reboot by adding an entry to the `/etc/hostname6.ip6.tun0` file.

The entry replicates the parameters that were passed to the `ifconfig` command in [Step 7](#).

- a. For example, on the `enigma` system, add the following entry to the `hostname6.ip6.tun0` file:

```

6000:6666::aaaa:1116 6000:3333::eeee:1113 \
tsrc 2001::aaaa:6666:6666 \
tdst 2001::eeee:3333:3333 \
encr_algs 3des encr_auth_algs md5 router up

```

- b. On the `partym` system, add the following entry to the `hostname6.ip6.tun0` file:

```

6000:3333::eeee:1113 6000:6666::aaaa:1116 \
tsrc 2001::eeee:3333:3333 \
tdst 2001::aaaa:6666:6666 \

```

```
encr_algs 3des encr_auth_algs md5 router up
```

12. On each system, configure the interface files to pass the correct parameters to the routing daemon.

a. On the enigma system, modify the `/etc/hostname6.interface` files.

```
# cat enigma hostname6.hme0
6000:6666::aaaa:1116 inet6 private

# cat enigma hostname6.hme1
2001::aaaa:6666:6666 inet6 router
```

b. On the partym system, modify the `/etc/hostname6.interface` files.

```
# cat partym hostname6.hme0
6000:3333::eeee:1113 inet6 private

# cat partym hostname6.hme1
2001::eeee:3333:3333 inet6 router
```

13. On each system, run a routing protocol.

```
# routeadm -e ipv6-routing
# routeadm -u
```

▼ How to Generate Random Numbers on a Solaris System

If you are entering keys manually, the keying material should be random. The format for keying material is hexadecimal.

If your site has a random number generator, use that generator. Otherwise, you can use the `od` command with the `/dev/random` Solaris device as input. For more information, see the `od(1)` man page.

Steps 1. Generate random numbers in hexadecimal format.

```
% od -x|-X -A n file | head -n
```

`-x` Displays the octal dump in hexadecimal format. Hexadecimal format is useful for keying material. The hexadecimal is printed in 4-character chunks.

`-X` Displays the octal dump in hexadecimal format. The hexadecimal is printed in 8-character chunks.

`-A n` Removes the input offset base from the display.

`file` Serves as a source for random numbers.

`head -n` Restricts the display to the first `n` lines of output.

2. Combine the output to create a key of the appropriate length.

Remove the spaces between the numbers on one line to create a 32-character key. A 32-character key is 128 bits. For a security parameter index (SPI), you should use an 8-character key. The key should use the 0x prefix.

Example 19–3 Generating Key Material for IPsec

The following example displays two lines of keys in groups of eight hexadecimal characters each.

```
% od -x -A n /dev/random | head -2
d54d1536 4a3e0352 0faf93bd 24fd6cad
8ecc2670 f3447465 20db0b0c c83f5a4b
```

By combining the four numbers on the first line, you can create a 32-character key. An 8-character number that is preceded by 0x provides a suitable SPI value, for example, 0xf3447465.

The following example displays two lines of keys in groups of four hexadecimal characters each.

```
% od -x -A n /dev/random | head -2
34ce 56b2 8b1b 3677 9231 42e9 80b0 c673
2f74 2817 8026 df68 12f4 905a db3d ef27
```

By combining the eight numbers on the first line, you can create a 32-character key.

▼ How to Manually Create IPsec Security Associations

Note – You manually manage keying material for a non-global zone from the global zone. You cannot use IKE to manage keys for a non-global zone.

The following procedure provides the keying material for the procedure, [“How to Secure Traffic Between Two Systems With IPsec”](#) on page 445.

Steps 1. **Generate the keying material for the SAs.**

You need three hexadecimal random numbers for outbound traffic and three hexadecimal random numbers for inbound traffic. Therefore, one system needs to generate the following numbers:

- Two hexadecimal random numbers as the value for the `spi` keyword. One number is for outbound traffic. One number is for inbound traffic. Each number can be up to eight characters long.
- Two hexadecimal random numbers for the MD5 algorithm for AH. Each number must be 32 characters long. One number is for `dst` `enigma`. One number is for `dst` `partym`.
- Two hexadecimal random numbers for the 3DES algorithm for ESP. For a 192-bit key, each number must be 48 characters long. One number is for `dst` `enigma`. One number is for `dst` `partym`.

If you have a random number generator at your site, use the generator. You can also use the `od` command. See [“How to Generate Random Numbers on a Solaris System”](#) on page 460 for the procedure.

2. On the system console on one of the systems, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

3. Enable the `ipseckey` command mode:

```
# ipseckey
```

```
>
```

The `>` prompt indicates that you are in `ipseckey` command mode.

4. If you are replacing existing SAs, flush the current SAs.

```
> flush
```

```
>
```

To prevent an adversary from having time to break your SAs, you need to replace the keying material.

Note – You must coordinate key replacement on communicating systems. When you replace the SAs on one system, the SAs must also be replaced on the remote system.

5. To create SAs, type the following command.

```
> add protocol spi random-hex-string \  
src addr dst addr2 \  
protocol-prefix_alg protocol-algorithm \  
protocol-prefixkey random-hex-string-of-algorithm-specified-length
```

You also use this syntax to replace SAs that you have just flushed.

protocol

Specifies either esp or ah.

random-hex-string

Specifies a random number of up to eight characters in hexadecimal format. Precede the characters with 0x. If you enter more numbers than the security parameter index (SPI) accepts, the system ignores the extra numbers. If you enter fewer numbers than the SPI accepts, the system pads your entry.

addr

Specifies the IP address of one system.

addr2

Specifies the IP address of the peer system of *addr*.

protocol-prefix

Specifies one of encr or auth. The encr prefix is used with the esp protocol. The auth prefix is used with the ah protocol. The option encr_auth_alg is used with the esp protocol.

protocol-algorithm

Specifies an algorithm for ESP or AH. Each algorithm requires a key of a specific length.

Authentication algorithms include MD5 and SHA. Encryption algorithms include 3DES and AES.

random-hex-string-of-algorithm-specified-length

Specifies a random hexadecimal number of the length that is required by the algorithm. For example, the MD5 algorithm requires a 32-character string for its 128-bit key. The 3DES algorithm requires a 48-character string for its 192-bit key.

a. For example, on the enigma system, protect outbound packets.

Use the random numbers that you generated in [Step 1](#).

```
> add esp spi 0x8bcd1407 \  
src 192.168.116.16 dst 192.168.13.213 \  
encr_alg 3des \  
encrkey d41fb74470271826a8e7a80d343cc5aae9e2a7f05f13730d  
  
> add ah spi 0x18907dae \  
src 192.168.116.16 dst 192.168.13.213 \  
auth_alg md5 \  
authkey e896f8df7f78d6cab36c94ccf293f031  
  
>
```

Note – The peer system must use the same keying material.

- b. Still in `ipseckey` command mode on the enigma system, protect inbound packets.

Type the following commands to protect the packets:

```
> add esp spi 0x122a43e4 \  
src 192.168.13.213 dst 192.168.116.16 \  
encr_alg 3des \  
encrkey dd325c5c137fb4739a55c9b3a1747baa06359826a5e4358e  
  
> add ah spi 0x91825a77 \  
src 192.168.13.213 dst 192.168.116.16 \  
auth_alg md5 \  
authkey ad9ced7ad5f255c9a8605fba5eb4d2fd  
  
>
```

Note – The keys and SPI can be different for each SA. You *should* assign different keys and a different SPI for each SA.

6. To exit `ipseckey` command mode, press Control-D or type quit.
7. To ensure that the keying material is available to IPsec at reboot, add the keying material to the `/etc/inet/secret/ipseckey` file.

The lines of the `/etc/inet/secret/ipseckey` file are identical to the command line language.

- a. For example, the `/etc/inet/secret/ipseckey` file on the enigma system would appear similar to the following:

```
# ipseckey - This file takes the file format documented in  
# ipseckey(1m).  
# Note that naming services might not be available when this file  
# loads, just like ipsecinit.conf.  
#  
# for outbound packets on enigma  
add esp spi 0x8bcd1407 \  
src 192.168.116.16 dst 192.168.13.213 \  
encr_alg 3des \  
encrkey d41fb74470271826a8e7a80d343cc5aae9e2a7f05f13730d  
#  
add ah spi 0x18907dae \  
src 192.168.116.16 dst 192.168.13.213 \  
auth_alg md5 \  
authkey e896f8df7f78d6cab36c94ccf293f031  
#
```



```

# for inbound packets
add esp spi 0x122a43e4 \
  src 192.168.13.213 dst 192.168.116.16 \
  encr_alg 3des \
  encrkey dd325c5c137fb4739a55c9b3a1747baa06359826a5e4358e
#
add ah spi 0x91825a77 \
  src 192.168.13.213 dst 192.168.116.16 \
  auth_alg md5 \
  authkey ad9ced7ad5f255c9a8605fba5eb4d2fd

```

b. Protect the file with read-only permissions.

```
# chmod 400 /etc/inet/secret/ipseckeys
```

8. Repeat Step 2 through Step 7 on the partym system.

Use the same keying material that was used on enigma.

The keying material on the two systems *must* be identical. As shown in the following example, only the comments in the `ipseckeys` file differ. The comments differ because `dst enigma` is inbound on the `enigma` system, and outbound on the `partym` system.

```

# partym ipseckeys file
#
# for inbound packets
add esp spi 0x8bcd1407 \
  src 192.168.116.16 dst 192.168.13.213 \
  encr_alg 3des \
  encrkey d41fb74470271826a8e7a80d343cc5aae9e2a7f05f13730d
#
add ah spi 0x18907dae \
  src 192.168.116.16 dst 192.168.13.213 \
  auth_alg md5 \
  authkey e896f8df7f78d6cab36c94ccf293f031
#
# for outbound packets
add esp spi 0x122a43e4 \
  src 192.168.13.213 dst 192.168.116.16 \
  encr_alg 3des \
  encrkey dd325c5c137fb4739a55c9b3a1747baa06359826a5e4358e
#
add ah spi 0x91825a77 \
  src 192.168.13.213 dst 192.168.116.16 \
  auth_alg md5 \
  authkey ad9ced7ad5f255c9a8605fba5eb4d2fd

```

▼ How to Verify That Packets Are Protected With IPsec

To verify that packets are protected, test the connection with the `snoop` command. The following prefixes can appear in the `snoop` output:

- AH: Prefix indicates that AH is protecting the headers. You see AH: if you used `auth_alg` to protect the traffic.
- ESP: Prefix indicates that encrypted data is being sent. You see ESP: if you used `encr_auth_alg` or `encr_alg` to protect the traffic.

Before You Begin You must be superuser or have assumed an equivalent role to create the snoop output. You must have access to both systems to test the connection.

Steps 1. On one system, such as `partym`, become superuser.

```
% suPassword:      Type root password
#
```

2. From the `partym` system, prepare to snoop packets from a remote system.

In a terminal window on `partym`, snoop the packets from the `enigma` system.

```
# snoop -v enigma
Using device /dev/hme (promiscuous mode)
```

3. Send a packet from the remote system.

In another terminal window, remotely log in to the `enigma` system. Provide your password. Then, become superuser and send a packet from the `enigma` system to the `partym` system. The packet should be captured by the `snoop -v enigma` command.

```
% rlogin enigma
Password:          Type your password
% su
Password:          Type root password
# ping partym
```

4. Examine the snoop output.

On the `partym` system, you should see output that includes AH and ESP information after the initial IP header information. AH and ESP information that resembles the following shows that packets are being protected:

```
IP:   Time to live = 64 seconds/hops
IP:   Protocol = 51 (AH)
IP:   Header checksum = 4e0e
IP:   Source address = 192.168.116.16, enigma
IP:   Destination address = 192.168.13.213, partym
IP:   No options
IP:
AH:   ----- Authentication Header -----
AH:
AH:   Next header = 50 (ESP)
AH:   AH length = 4 (24 bytes)
AH:   <Reserved field = 0x0>
AH:   SPI = 0xb3a8d714
AH:   Replay = 52
AH:   ICV = c653901433ef5a7d77c76eaa
```

```

AH:
ESP: ----- Encapsulating Security Payload -----
ESP:
ESP: SPI = 0xd4f40a61
ESP: Replay = 52
ESP:      ....ENCRYPTED DATA....

ETHER: ----- Ether Header -----
...

```

▼ How to Create a Role for Configuring Network Security

If you are using role-based access control (RBAC) to administer your systems, you use this procedure to provide a network management or network security role.

Steps 1. Find the Network rights profiles in the local `prof_attr` database.

```

% cd /etc/security
% grep Network prof_attr
Network Management:::Manage the host and network configuration ...
Network Security:::Manage network and host security ...
System Administrator:::...Network Management...

```

The Network Management profile is a supplementary profile in the System Administrator profile. If you have included the System Administrator rights profile in a role, then that role can execute the commands in the Network Management profile.

2. Determine which commands are in the Network Management rights profile.

```

% grep "Network Management" /etc/security/exec_attr
Network Management:solaris:cmd:::/usr/sbin/ifconfig:privs=sys_net_config
...
Network Management:suser:cmd:::/usr/sbin/snoop:uid=0

```

The solaris policy commands run with privilege (`privs=sys_net_config`).
The suser policy commands run as superuser (`uid=0`).

3. Determine which commands are in the Network Security rights profile.

```

% grep "Network Security" /etc/security/exec_attr
...
Network Security:solaris:cmd:::/usr/sbin/ipsecconf:privs=sys_net_config
...
Network Security:solaris:cmd:::/usr/sbin/ipseckey:privs=sys_net_config
...

```

4. Create a role that includes the Network Security and the Network Management rights profiles.

A role with both profiles can execute the `ifconfig`, `snoop`, `ipsecconf`, and `ipseckey` commands, among others, with appropriate privilege.

To create the role, assign the role to a user, and register the changes with the name service, see "Configuring RBAC (Task Map)" in *System Administration Guide: Security Services*.

IP Security Architecture (Reference)

This chapter contains the following reference information:

- “[ipseccconf Command](#)” on page 469
- “[ipseccinit.conf File](#)” on page 470
- “[ipseccalgs Command](#)” on page 472
- “[Security Associations Database for IPsec](#)” on page 472
- “[Utilities for Key Generation in IPsec](#)” on page 473
- “[IPsec Extensions to Other Utilities](#)” on page 474

For instructions on how to implement IPsec on your network, see [Chapter 19](#). For an overview of IPsec, see [Chapter 18](#).

ipseccconf Command

You use the `ipseccconf` command to configure the IPsec policy for a host. When you run the command to configure the policy, the system creates a temporary file that is named `ipseccpolicy.conf`. This file holds the IPsec policy entries that were set in the kernel by the `ipseccconf` command. The system uses the in-kernel IPsec policy entries to check the policy on all outbound and inbound IP datagrams. Forwarded datagrams are not subjected to policy checks that are added by using this command. The `ipseccconf` command also configures the security policy database (SPD).

- For information on how to protect forwarded packets, see the `ifconfig(1M)` and `tun(7M)` man pages.
- For IPsec policy options, see the `ipseccconf(1M)` man page.
- For instructions on how to use the `ipseccconf` command to protect traffic between systems, see “[Configuring IKE \(Task Map\)](#)” on page 485.

You must become superuser or assume an equivalent role to invoke the `ipseccconf` command. The command accepts entries that protect traffic in both directions. The command also accepts entries that protect traffic in only one direction.

Policy entries with a format of local address and remote address can protect traffic in both directions with a single policy entry. For example, entries that contain the patterns `laddr host1` and `raddr host2` protect traffic in both directions, if no direction is specified for the named host. Thus, you need only one policy entry for each host.

Policy entries with a format of source address to destination address protect traffic in only one direction. For example, a policy entry of the pattern `saddr host1 daddr host2` protects inbound traffic or outbound traffic, not both directions. Thus, to protect traffic in both directions, you need to pass the `ipseccconf` command another entry, as in `saddr host2 daddr host1`.

The `ipsecpolicy.conf` file is deleted when the system shuts down. To ensure that the IPsec policy is active when the machine boots, you can create an IPsec policy file, `/etc/inet/ipsecinit.conf`. This file is read when the network services are started. For instructions on how to create an IPsec policy file, see [“Configuring IPsec \(Task Map\)” on page 443](#).

ipseccinit.conf File

To invoke IPsec security policies when you start the Solaris Operating System, you create a configuration file to initialize IPsec with your specific IPsec entries. You should name the file `/etc/inet/ipsecinit.conf`. See the `ipseccconf(1M)` man page for details about policy entries and their format. After policies are configured, you can use the `ipseccconf` command to view or modify the existing configuration.

Sample ipsecinit.conf File

The Solaris software includes a sample IPsec policy file, `ipseccinit.sample`. You can use the file as a template to create your own `ipseccinit.conf` file. The `ipseccinit.sample` file contains the following examples:

```
#
# For example,
#
#   {rport 23} ipsec {encr_algs des encr_auth_algs md5}
#
# will protect the telnet traffic originating from the host with ESP using
# DES and MD5. Also:
#
#   {raddr 10.5.5.0/24} ipsec {auth_algs any}
#
# will protect traffic to or from the 10.5.5.0 subnet with AH
# using any available algorithm.
```

```

#
#
# To do basic filtering, a drop rule may be used. For example:
#
#   {lport 23 dir in} drop {}
#   {lport 23 dir out} drop {}
#
# will disallow any remote system from telnetting in.
#
# If you are using IPv6, it may be useful to bypass neighbor discovery
# to allow in.iked to work properly with on-link neighbors. To do that,
# add the following lines:
#
#       {ulp ipv6-icmp type 133-137 dir both } pass { }
#
# This will allow neighbor discovery to work normally.

```

Security Considerations for `ipsecinit.conf` and `ipseccnf`

Use extreme caution if transmitting a copy of the `ipsecinit.conf` file over a network. An adversary can read a network-mounted file as the file is being read. If, for example, the `/etc/inet/ipsecinit.conf` file is accessed or is copied from an NFS-mounted file system, an adversary can change the policy that is contained in the file.

Ensure that you set up IPsec policies before starting any communications, because existing connections might be affected by the addition of new policy entries. Similarly, do not change policies in the middle of a communication.

Specifically, IPsec policy cannot be changed for SCTP, TCP, or UDP sockets on which a `connect()` or `accept()` function call has been issued. A socket whose policy cannot be changed is called a *latched socket*. New policy entries do not protect sockets that are already latched. For more information, see the `connect(3SOCKET)` and `accept(3SOCKET)` man pages.

Protect your naming system. If the following two conditions are met, then your host names are no longer trustworthy:

- Your source address is a host that can be looked up over the network.
- Your naming system is compromised.

Security weaknesses often arise from the misapplication of tools, not from the actual tools. You should be cautious when using the `ipseccnf` command. Use a console or other hard-connected TTY for the safest mode of operation.

ipsecalgs Command

The Solaris cryptographic framework provides authentication and encryption algorithms to IPsec. You use the `ipsecalgs` command to query and modify the list of protocols and the list of algorithms that IPsec supports. The `ipsecalgs` command stores this information in tabular format in the IPsec protocols and algorithms file, `/etc/inet/ipsecalgs`. This file must never be edited manually.

The valid IPsec protocols and algorithms are described by the ISAKMP [domain of interpretation \(DOI\)](#), which is covered by RFC 2407. In a general sense, a DOI defines data formats, network traffic exchange types, and conventions for naming security-relevant information. Security policies, cryptographic algorithms, and cryptographic modes are examples of security-relevant information.

Specifically, the ISAKMP DOI defines the naming and numbering conventions for the valid IPsec algorithms and for their protocols, `PROTO_IPSEC_AH` and `PROTO_IPSEC_ESP`. Each algorithm is associated with exactly one protocol. These ISAKMP DOI definitions are in the `/etc/inet/ipsecalgs` file. The algorithm and protocol numbers are defined by the Internet Assigned Numbers Authority (IANA). The `ipsecalgs` command makes the list of algorithms for IPsec extensible.

For more information on the algorithms, refer to the `ipsecalgs(1M)` man page. For more information on the Solaris cryptographic framework, see Chapter 13, “Solaris Cryptographic Framework (Overview),” in *System Administration Guide: Security Services*.

Security Associations Database for IPsec

Information on key material for IPsec security services is maintained in a security associations database (SADB). Security associations (SAs) protect inbound packets and outbound packets. The SADB is maintained by a user process, or possibly multiple cooperating processes, that send messages over a special kind of socket. This method of maintaining SADB is analogous to the method that is described in the `route(7P)` man page. Only superuser or a user who has assumed an equivalent role can access the database.

The `in.iked` daemon and the `ipseckey` command use the `pf_key` socket interface to maintain SADB. For more information on how SADB handles requests and messages, see the `pf_key(7P)` man page.

Utilities for Key Generation in IPsec

The IKE protocol provides automatic key management for IPv4 and IPv6 addresses. See [Chapter 22](#) for instructions on how to set up IKE. The manual keying utility is the `ipseckey` command, which is described in the `ipseckey(1M)` man page.

You use the `ipseckey` command to manually populate the security association databases (SADBs) when automated key management is not used. When you invoke the `ipseckey` command with no arguments, the command enters an interactive mode and displays a prompt that enables you to make entries. Some commands require an explicit security association (SA) type, while others permit you to specify the SA type and act on all SA types.

While the `ipseckey` command has only a limited number of general options, the command supports a rich command language. You can specify that requests be delivered by means of a programmatic interface specific for manual keying. For additional information, see the `pf_key(7P)` man page.

Security Considerations for `ipseckey`

The `ipseckey` command enables superuser or a role with the Network Security profile to enter sensitive cryptographic keying information. If an adversary gains access to this information, the adversary can compromise the security of IPsec traffic. You should consider the following issues when you handle keying material and use the `ipseckey` command:

- Have you refreshed the keying material? Periodic key refreshment is a fundamental security practice. Key refreshment guards against potential weaknesses of the algorithm and keys, and limits the damage of an exposed key.
- Is the TTY going over a network? Is the `ipseckey` command in interactive mode?
 - In interactive mode, the security of the keying material is the security of the network path for this TTY's traffic. You should avoid using the `ipseckey` command over a clear-text telnet or rlogin session.
 - Even local windows might be vulnerable to attacks by a concealed program that reads window events.
- Have you used the `-f` option? Is the file being accessed over the network? Can the file be read by the world?
 - An adversary can read a network-mounted file as the file is being read. You should avoid using a world-readable file that contains keying material.
 - Protect your naming system. If the following two conditions are met, then your host names are no longer trustworthy:
 - Your source address is a host that can be looked up over the network.

- Your naming system is compromised.

Security weaknesses often arise from the misapplication of tools, not from the actual tools. You should be cautious when using the `ipseckey` command. Use a console or other hard-connected TTY for the safest mode of operation.

IPsec Extensions to Other Utilities

The `ifconfig` command has options to manage the IPsec policy on a tunnel interface. The `snoop` command can parse AH and ESP headers.

`ifconfig` Command and IPsec

To support IPsec, the following security options are available from the `ifconfig` command:

- `auth_algs`
- `encr_auth_algs`
- `encr_algs`

You must specify all IPsec security options for a tunnel in one invocation. For example, if you are using only ESP to protect traffic, you would configure the tunnel, `ip.tun0`, once with both security options, as in:

```
# ifconfig ip.tun0 ... encr_algs 3des encr_auth_algs md5
```

Similarly, an `ipsecinit.conf` entry would configure the tunnel once with both security options, as in:

```
# WAN traffic uses ESP with 3DES and MD5.
  {} ipsec {encr_algs 3des encr_auth_algs md5}
```

`auth_algs` Security Option

This option enables IPsec AH for a tunnel with a specified authentication algorithm. The `auth_algs` option has the following format:

```
auth_algs authentication-algorithm
```

For the algorithm, you can specify either a number or an algorithm name, including the parameter *any*, to express no specific algorithm preference. To disable tunnel security, specify the following option:

```
auth_algs none
```

For a list of available authentication algorithms, run the `ipsecalgs` command.

Note – The `auth_algs` option cannot work with NAT-Traversal. For more information, see [“IPsec and NAT Traversal” on page 437](#).

`encr_auth_algs` Security Option

This option enables IPsec ESP for a tunnel with a specified authentication algorithm. The `encr_auth_algs` option has the following format:

```
encr_auth_algs authentication-algorithm
```

For the algorithm, you can specify either a number or an algorithm name, including the parameter *any*, to express no specific algorithm preference. If you specify an ESP encryption algorithm, but you do not specify the authentication algorithm, the ESP authentication algorithm value defaults to the parameter *any*.

For a list of available authentication algorithms, run the `ipsecalgs` command.

`encr_algs` Security Option

This option enables IPsec ESP for a tunnel with a specified encryption algorithm. The `encr_algs` option has the following format:

```
encr_algs encryption-algorithm
```

For the algorithm, you can specify either a number or an algorithm name. To disable tunnel security, specify the following option:

```
encr_algs none
```

If you specify an ESP authentication algorithm, but not an encryption algorithm, ESP's encryption value defaults to the parameter *null*.

For a list of available encryption algorithms, run the `ipsecalgs` command.

`snoop` Command and IPsec

The `snoop` command can parse AH and ESP headers. Because ESP encrypts its data, the `snoop` command cannot see encrypted headers that are protected by ESP. AH does not encrypt data. Therefore, traffic that is protected by AH can be inspected with the `snoop` command. The `-v` option to the command shows when AH is in use on a packet. For more details, see the `snoop(1M)` man page.

For a sample of verbose `snoop` output on a protected packet, see [“How to Verify That Packets Are Protected With IPsec” on page 465](#).

Internet Key Exchange (Overview)

Internet Key Exchange (IKE) automates key management for IPsec. This chapter contains the following information about IKE:

- “Key Management With IKE” on page 477
- “IKE Key Negotiation” on page 478
- “IKE Configuration Choices” on page 480
- “IKE and Hardware Acceleration” on page 481
- “IKE and Hardware Storage” on page 481
- “IKE Utilities and Files” on page 482
- “Changes to IKE for the Solaris 10 Release” on page 483

For instructions on implementing IKE, see [Chapter 22](#). For reference information, see [Chapter 23](#). For information about IPsec, see [Chapter 18](#).

Key Management With IKE

The management of keying material for IPsec security associations (SAs) is called *key management*. Automatic key management requires a secure channel of communication for the creation, authentication, and exchange of keys. The Solaris Operating System uses Internet Key Exchange (IKE) to automate key management. IKE easily scales to provide a secure channel for a large volume of traffic. IPsec SAs on IPv4 and IPv6 packets can take advantage of IKE.

When IKE is used on a system with a Sun™ Crypto Accelerator 1000 board or a Sun Crypto Accelerator 4000 board, the public key operations can be offloaded to the accelerator. Operating system resources are not used for public key operations. When IKE is used on a system with a Sun Crypto Accelerator 4000 board, the certificates, public keys, and private keys can be stored on the board. Key storage that is off the system provides an additional layer of protection.

IKE Key Negotiation

The IKE daemon, `in.iked`, negotiates and authenticates keying material for SAs in a protected manner. The daemon uses random seeds for keys from internal functions provided by the Solaris Operating System. IKE provides perfect forward secrecy (PFS). In PFS, the keys that protect data transmission are not used to derive additional keys. Also, seeds used to create data transmission keys are not reused. See the `in.iked(1M)` man page.

When the IKE daemon discovers a remote system's public encryption key, the local system can then use that key. The system encrypts messages by using the remote system's public key. The messages can be read only by that remote system. The IKE daemon performs its job in two phases. The phases are called *exchanges*.

IKE Key Terminology

The following table lists terms that are used in key negotiation, provides their commonly used acronyms, and gives a definition and use for each term.

TABLE 21-1 Key Negotiation Terms, Acronyms, and Uses

Key Negotiation Term	Acronym	Definition and Use
Key exchange		The process of generating keys for asymmetric cryptographic algorithms. The two main methods are RSA protocols and the Diffie-Hellman protocol.
Diffie-Hellman protocol	DH	A key exchange protocol that involves key generation and key authentication. Often called <i>authenticated key exchange</i> .
RSA protocol	RSA	A key exchange protocol that involves key generation and key transport. The protocol is named for its three creators, Rivest, Shamir, and Adleman.
Perfect forward secrecy	PFS	Applies to authenticated key exchange only. PFS ensures that long-term secret material for keys does not compromise the secrecy of the exchanged keys from previous communications. In PFS, the key that is used to protect transmission of data is not used to derive additional keys. Also, the source of the key that is used to protect data transmission is never used to derive additional keys.

TABLE 21-1 Key Negotiation Terms, Acronyms, and Uses (Continued)

Key Negotiation Term	Acronym	Definition and Use
Oakley method		A method for establishing keys for Phase 2 in a secure manner. This protocol is analogous to the Diffie-Hellman method of key exchange. Similar to Diffie-Hellman, Oakley group key exchange involves key generation and key authentication. The Oakley method is used to negotiate PFS.

IKE Phase 1 Exchange

The Phase 1 exchange is known as *Main Mode*. In the Phase 1 exchange, IKE uses public key encryption methods to authenticate itself with peer IKE entities. The result is an Internet Security Association and Key Management Protocol (ISAKMP) security association (SA). An ISAKMP SA is a secure channel for IKE to negotiate keying material for the IP datagrams. Unlike IPsec SAs, the ISAKMP SAs are bidirectional, so only one security association is needed.

How IKE negotiates keying material in the Phase 1 exchange is configurable. IKE reads the configuration information from the `/etc/inet/ike/config` file. Configuration information includes the following:

- Global parameters, such as the names of public key certificates
- Whether perfect forward secrecy (PFS) is used
- The interfaces that are affected
- The security protocols and their algorithms
- The authentication method

The two authentication methods are preshared keys and public key certificates. The public key certificates can be self-signed. Or, the certificates can be issued by a [certificate authority \(CA\)](#) from a public key infrastructure (PKI) organization. Organizations include beTrusted, Entrust, GeoTrust, RSA Security, and Verisign.

IKE Phase 2 Exchange

The Phase 2 exchange is known as *Quick Mode*. In the Phase 2 exchange, IKE creates and manages the IPsec SAs between systems that are running the IKE daemon. IKE uses the secure channel that was created in the Phase 1 exchange to protect the transmission of keying material. The IKE daemon creates the keys from a random number generator by using the `/dev/random` device. The daemon refreshes the keys at a configurable rate. The keying material is available to algorithms that are specified in the configuration file for IPsec policy, `ipsecinit.conf`.

IKE Configuration Choices

The `/etc/inet/ike/config` configuration file contains IKE policy entries. For two IKE daemons to authenticate each other, the entries must be valid. Also, keying material must be available. The entries in the configuration file determine the method for using the keying material to authenticate the Phase 1 exchange. The choices are preshared keys or public key certificates.

The entry `auth_method preshared` indicates that preshared keys are used. Values for `auth_method` other than `preshared` indicate that public key certificates are to be used. Public key certificates can be self-signed, or the certificates can be installed from a PKI organization. For more information, see the `ike.config(4)` man page.

IKE With Preshared Keys

Preshared keys are created by an administrator on one system. The keys are then shared out of band with administrators of remote systems. You should take care to create large random keys and to protect the file and the out-of-band transmission. The keys are placed in the `/etc/inet/secret/ike.preshared` file on each system. The `ike.preshared` file is for IKE as the `ipseckey` file is for IPsec. Any compromise of the keys in the `ike.preshared` file compromises all keys that are derived from the keys in the file.

One system's preshared key must be identical to its remote system's key. The keys are tied to a particular IP address. Keys are most secure when one administrator controls the communicating systems. For more information, see the `ike.preshared(4)` man page.

IKE With Public Key Certificates

Public key certificates eliminate the need for communicating systems to share secret keying material out of band. Public keys use the [Diffie-Hellman protocol \(DH\)](#) for authenticating and negotiating keys. Public key certificates come in two flavors. The certificates can be self-signed, or the certificates can be certified by a [certificate authority \(CA\)](#).

Self-signed public key certificates are created by you, the administrator. The `ikecert certlocal -ks` command creates the private part of the public-private key pair for the system. You then get the self-signed certificate output in X.509 format from the remote system. The remote system's certificate is input to the `ikecert certdb` command for the public part of the key pair. The self-signed certificates reside in the `/etc/inet/ike/publickeys` directory on the communicating systems. When you use the `-T` option, the certificates reside on attached hardware.

Self-signed certificates are a halfway point between preshared keys and CAs. Unlike preshared keys, a self-signed certificate can be used on a mobile machine or on a system that might be renumbered. To self-sign a certificate for a system without a fixed number, use a DNS (`www.example.org`) or EMAIL (`root@domain.org`) alternative name.

Public keys can be delivered by a PKI or a CA organization. You install the public keys and their accompanying CAs in the `/etc/inet/ike/publickeys` directory. When you use the `-T` option, the certificates reside on attached hardware. Vendors also issue certificate revocation lists (CRLs). Along with installing the keys and CAs, you are responsible for installing the CRL in the `/etc/inet/ike/crls` directory.

CAs have the advantage of being certified by an outside organization, rather than by the site administrator. In a sense, CAs are notarized certificates. As with self-signed certificates, CAs can be used on a mobile machine or on a system that might be renumbered. Unlike self-signed certificates, CAs can very easily scale to protect a large number of communicating systems.

IKE and Hardware Acceleration

IKE algorithms are computationally expensive, particularly in the Phase 1 exchange. Systems that handle a large number of exchanges can use a Sun Crypto Accelerator 1000 board to handle the public key operations. The Sun Crypto Accelerator 4000 board can also be used to handle expensive Phase 1 computations.

For information on how to configure IKE to offload its computations to the accelerator board, see [“How to Configure IKE to Find the Sun Crypto Accelerator 1000 Board”](#) on page 521. For information on how to store keys, see [“How to Configure IKE to Find the Sun Crypto Accelerator 4000 Board”](#) on page 522.

IKE and Hardware Storage

Public key certificates, private keys, and public keys can be stored on a Sun Crypto Accelerator 4000 board. For *RSA* encryption, the board supports keys up to 2048 bits. For *DSA* encryption, the board supports keys up to 1024 bits.

For information on how to configure IKE to access the board, see [“How to Configure IKE to Find the Sun Crypto Accelerator 1000 Board”](#) on page 521. For information on how to add certificates and public keys to the board, see [“How to Generate and Store Public Key Certificates on Hardware”](#) on page 506.

IKE Utilities and Files

The following table summarizes the configuration files for IKE policy, the storage locations for IKE keys, and the various commands that implement IKE.

TABLE 21-2 IKE Configuration Files, Key Storage Locations, and Commands

File, Command, or Location	Description	For More Information
<code>/usr/lib/inet/in.iked daemon</code>	Internet Key Exchange (IKE) daemon. Activates automated key management.	<code>in.iked(1M)</code>
<code>/usr/sbin/ikeadm command</code>	IKE administration command for viewing and modifying the IKE policy.	<code>ikeadm(1M)</code>
<code>/usr/sbin/ikecert command</code>	Certificate database management command for manipulating local databases that hold public key certificates. The databases can also be stored on an attached Sun Crypto Accelerator 4000 board.	<code>ikecert(1M)</code>
<code>ike/config file</code>	Configuration file for the IKE policy in the <code>/etc/inet</code> directory. Contains the site's rules for matching inbound IKE requests and preparing outbound IKE requests. If this file exists, the <code>in.iked</code> daemon starts automatically at boot time.	<code>ike.config(4)</code>
<code>ike.preshared file</code>	Preshared keys file in the <code>/etc/inet/secret</code> directory. Contains secret keying material for authentication in the Phase 1 exchange. Used when configuring IKE with preshared keys.	<code>ike.preshared(4)</code>
<code>ike.privatekeys directory</code>	Private keys directory in the <code>/etc/inet/secret</code> directory. Contains the private keys that are part of a public-private key pair.	<code>ikecert(1M)</code>
<code>publickeys directory</code>	Directory in the <code>/etc/inet/ike</code> directory that holds public keys and certificate files. Contains the public key part of a public-private key pair.	<code>ikecert(1M)</code>
<code>crls directory</code>	Directory in the <code>/etc/inet/ike</code> directory that holds revocation lists for public keys and certificate files.	<code>ikecert(1M)</code>
Sun Crypto Accelerator 1000 board	Hardware that accelerates public key operations by offloading the operations from the operating system.	<code>ikecert(1M)</code>
Sun Crypto Accelerator 4000 board	Hardware that accelerates public key operations by offloading the operations from the operating system. The board also stores public keys, private keys, and public key certificates.	<code>ikecert(1M)</code>

Changes to IKE for the Solaris 10 Release

Since the Solaris 9 release, IKE includes the following functionality:

- IKE can be used to automate key exchange for IPsec over IPv6 networks. For more information, see [“Key Management With IKE” on page 477](#).

Note – IKE cannot be used to manage keys for IPsec in a non-global zone.

- Public key operations in IKE can be accelerated by a Sun Crypto Accelerator 1000 board or a Sun Crypto Accelerator 4000 board. The operations are offloaded to the board. The offloading accelerates encryption, thereby reducing demands on operating system resources. For more information, see [“IKE and Hardware Acceleration” on page 481](#). For procedures, see [“Configuring IKE to Find Attached Hardware \(Task Map\)” on page 520](#).
- Public key certificates, private keys, and public keys can be stored on a Sun Crypto Accelerator 4000 board. For more information on key storage, see [“IKE and Hardware Storage” on page 481](#).
- IKE can be used to automate key exchange for IPsec from behind a NAT box. The traffic must use an IPv4 network. Also, the NAT-traversing IPsec ESP keys cannot be accelerated by hardware. For more information, see [“IPsec and NAT Traversal” on page 437](#). For procedures, see [“Configuring IKE for Mobile Systems \(Task Map\)” on page 512](#).
- Retransmission parameters and packet timeout parameters have been added to the `/etc/inet/ike/config` file. These parameters tune the IKE Phase 1 (Main Mode) negotiation to handle network interference, heavy network traffic, and interoperation with platforms that have different implementations of the IKE protocol. For details about the parameters, see the `ike.config(4)` man page. For procedures, see [“Changing IKE Transmission Parameters \(Task Map\)” on page 523](#).

Configuring IKE (Tasks)

This chapter describes how to configure IKE for your systems. After IKE is configured, it automatically generates keying material for IPsec on your network. This chapter contains the following information:

- “Configuring IKE (Task Map)” on page 485
- “Configuring IKE With Preshared Keys (Task Map)” on page 486
- “Configuring IKE With Public Key Certificates (Task Map)” on page 496
- “Configuring IKE for Mobile Systems (Task Map)” on page 512
- “Configuring IKE to Find Attached Hardware (Task Map)” on page 520
- “Changing IKE Transmission Parameters (Task Map)” on page 523

For overview information about IKE, see [Chapter 21](#). For reference information about IKE, see [Chapter 23](#). For more procedures, see the Examples sections of the `ikeadm(1M)`, `ikecert(1M)`, and `ike.config(4)` man pages.

Configuring IKE (Task Map)

You can use preshared keys, self-signed certificates, and certificates from a Certificate Authority (CA) to authenticate IKE. A rule links the particular IKE authentication method with the end points that are being protected. Therefore, you can use one or all IKE authentication methods on a system. A pointer to a PKCS #11 library enables certificates to use an attached hardware accelerator.

After configuring IKE, complete the IPsec task that uses the IKE configuration. The following table refers you to task maps that focus on a specific IKE configuration.

Task	Description	For Instructions
Configure IKE with preshared keys	Protects communications between two systems by having the systems share a secret key.	"Configuring IKE With Preshared Keys (Task Map)" on page 486
Configure IKE with public key certificates	Protects communications with public key certificates. The certificates can be self-signed, or they can be vouched for by a PKI organization.	"Configuring IKE With Public Key Certificates (Task Map)" on page 496
Cross a NAT boundary	Configures IPsec and IKE to communicate with a mobile system	"Configuring IKE for Mobile Systems (Task Map)" on page 512
Configure IKE to generate and store public key certificates on attached hardware	Enables a Sun Crypto Accelerator 1000 board or a Sun Crypto Accelerator 4000 board to accelerate IKE operations. Also enables the Sun Crypto Accelerator 4000 board to store public key certificates.	"Configuring IKE to Find Attached Hardware (Task Map)" on page 520
Tune Phase 1 key negotiation parameters	Changes the timing of IKE key negotiations.	"Changing IKE Transmission Parameters (Task Map)" on page 523

Configuring IKE With Preshared Keys (Task Map)

The following table points to procedures to configure and maintain IKE with preshared keys.

Task	Description	For Instructions
Configure IKE with preshared keys	Creates an IKE policy file and one key to be shared.	"How to Configure IKE With Preshared Keys" on page 487
Refresh preshared keys on a running IKE system	Adds fresh keying material for IKE on communicating systems.	"How to Refresh IKE Preshared Keys" on page 490
Add preshared keys to a running IKE system	Adds a new IKE policy entry and new keying material to a system that is currently enforcing IKE policy.	"How to Add an IKE Preshared Key for a New Policy Entry in ipsecinit.conf" on page 491
Check that preshared keys are identical	Displays the preshared keys on both systems to see that the keys are identical.	"How to Verify That IKE Preshared Keys Are Identical" on page 494

Configuring IKE With Preshared Keys

Preshared keys is the simplest authentication method for IKE. If you are configuring two systems to use IKE, and you are the administrator for both of the systems, using preshared keys is a good choice. However, unlike public key certificates, preshared keys are tied to particular IP addresses. Preshared keys cannot be used with mobile systems or systems that might be renumbered. Also, when you use preshared keys, you cannot offload IKE computations to attached hardware.

▼ How to Configure IKE With Preshared Keys

The IKE implementation offers algorithms whose keys vary in length. The key length that you choose is determined by site security. In general, longer keys provide more security than shorter keys.

These procedures use the system names `enigma` and `partym`. Substitute the names of your systems for the names `enigma` and `partym`.

Steps 1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **On each system, copy the file `/etc/inet/ike/config.sample` to the file `/etc/inet/ike/config`.**

3. **Enter rules and global parameters in the `ike/config` file on each system.**

The rules and global parameters in this file should permit the IPsec policy in the system’s `ipsecinit.conf` file to succeed. The following `ike/config` examples work with the `ipsecinit.conf` examples in “How to Secure Traffic Between Two Systems With IPsec” on page 445.

a. **For example, modify the `/etc/inet/ike/config` file on the `enigma` system:**

```
### ike/config file on enigma, 192.168.116.16
```

```

## Global parameters
#
## Phase 1 transform defaults
p1_lifetime_secs 14400
p1_nonce_len 40
#
## Defaults that individual rules can override.
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2
#
## The rule to communicate with partym
# Label must be unique
{ label "enigma-partym"
  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  p1_xform
  { auth_method preshared oakley_group 5 auth_alg md5 encr_alg 3des }
  p2_pfs 5
}

```

Note – All arguments to the `auth_method` parameter must be on the same line.

b. Modify the `/etc/inet/ike/config` file on the partym system:

```

### ike/config file on partym, 192.168.13.213
## Global Parameters
#
p1_lifetime_secs 14400
p1_nonce_len 40
#
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 2

## The rule to communicate with enigma
# Label must be unique
{ label "partym-enigma"
  local_addr 192.168.13.213
  remote_addr 192.168.116.16
  p1_xform
  { auth_method preshared oakley_group 5 auth_alg md5 encr_alg 3des }
  p2_pfs 5
}

```

4. On each system, check the validity of the file.

```
# /usr/lib/inet/in.iked -c -f /etc/inet/ike/config
```

5. Generate random numbers for use as keying material.

If your site has a random number generator, use that generator. On a Solaris system, you can use the `od` command. For example, the following command prints two lines of hexadecimal numbers:

```
% od -x -A n /dev/random | head -2
      f47cb0f4 32e14480 951095f8 2b735ba8
      0a9467d0 8f92c880 68b6a40e 0efe067d
```

For an explanation of the `od` command, see [“How to Generate Random Numbers on a Solaris System” on page 460](#) and the `od(1)` man page.

6. From the output of Step 5, construct one key.

```
f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
```

The authentication algorithm in this procedure is MD5, as shown in [Step 3](#). The size of the hash, that is, the size of the authentication algorithm’s output, determines the minimum recommended size of a preshared key. The output of the MD5 algorithm is 128 bits, or 32 characters. The example key is 56 characters long, which provides additional keying material for IKE to use.

7. Create the file `/etc/inet/secret/ike.preshared` on each system.

Put the preshared key in each file.

a. For example, on the `enigma` system, the `ike.preshared` file would appear similar to the following:

```
# ike.preshared on enigma, 192.168.116.16
#...
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.13.213
  # enigma and partym’s shared key in hex (192 bits)
  key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
}
```

b. On the `partym` system, the `ike.preshared` file would appear similar to the following:

```
# ike.preshared on partym, 192.168.13.213
#...
{ localidtype IP
  localid 192.168.13.213
  remoteidtype IP
  remoteid 192.168.116.16
  # partym and enigma’s shared key in hex (192 bits)
  key f47cb0f432e14480951095f82b735ba80a9467d08f92c88068b6a40e
}
```

Note – The preshared keys on each system must be identical.

▼ How to Refresh IKE Preshared Keys

This procedure assumes that you want to replace an existing preshared key at regular intervals without rebooting. If you use a strong encryption algorithm, such as 3DES or Blowfish, you might want to refresh keys just before you reboot both systems.

- Steps**
1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Generate random numbers and construct a key of the appropriate length.**
For details, see “How to Generate Random Numbers on a Solaris System” on page 460.
3. **Replace the current key with a new key.**
For example, on the hosts `enigma` and `partym`, you would replace the value of `key` in the `/etc/inet/secret/ike.preshared` file with a new number of the same length.
4. **Check the privilege level of the `in.iked` daemon.**

```
# /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

You can change the keying material if the command returns a privilege level of `0x1` or `0x2`. Level `0x0` does not permit operations to modify or view keying material. By default, the `in.iked` daemon runs at the `0x0` level of privilege.

- **If the privilege level is `0x0`, kill and restart the daemon.**

When the daemon restarts, it reads the new version of the `ike.preshared` file.

```
# pkill in.iked
# /usr/lib/inet/in.iked
```

- **If the privilege level is `0x1` or `0x2`, read in the new version of the `ike.preshared` file.**

```
# ikeadm read preshared
```

▼ How to Add an IKE Preshared Key for a New Policy Entry in `ipsecinit.conf`

You must have one preshared key for every policy entry in the `ipsecinit.conf` file. If you add a new policy entry while IPsec and IKE are running, the `in.iked` daemon can read in new keys.

Before You Begin

This procedure assumes the following:

- The `enigma` system is set up as described in “How to Configure IKE With Preshared Keys” on page 487.
- The `enigma` system is going to protect its traffic with a new system, `ada`.
- The `in.iked` daemon is running on both systems.
- The systems’ interfaces are included as entries in the `/etc/hosts` file on both systems. The following entry is an example.

```
192.168.15.7 ada
192.168.116.16 enigma
```

This procedure also works with an IPv6 address in the `/etc/inet/ipnodes` file.

- You have added a new policy entry to the `/etc/inet/ipsecinit.conf` file on both systems. The entries appear similar to the following:

```
# ipsecinit.conf file for enigma
{laddr enigma raddr ada} ipsec {auth_algs any encr_algs any sa shared}

# ipsecinit.conf file for ada
{laddr ada raddr enigma} ipsec {auth_algs any encr_algs any sa shared}
```

- Steps**
1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Create a rule for IKE to manage the keys for `enigma` and `ada`.**

- a. For example, the rule in the `/etc/inet/ike/config` file on the enigma system appears similar to the following:

```
### ike/config file on enigma, 192.168.116.16
...
## The rule to communicate with ada

{label "enigma-to-ada"
 local_addr 192.168.116.16
 remote_addr 192.168.15.7
 p1_xform
 {auth_method preshared oakley_group 5 auth_alg md5 encr_alg blowfish}
 p2_pfs 5
 }
```

- b. The rule in the `/etc/inet/ike/config` file on the ada system appears similar to the following:

```
### ike/config file on ada, 192.168.15.7
...
## The rule to communicate with enigma

{label "ada-to-enigma"
 local_addr 192.168.15.7
 remote_addr 192.168.116.16
 p1_xform
 {auth_method preshared oakley_group 5 auth_alg md5 encr_alg blowfish}
 p2_pfs 5
 }
```

3. Check the privilege level of the `in.iked` daemon.

```
# /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

- If the privilege level is `0x1` or `0x2`, continue with the next step.
- If the privilege level is `0x0`, stop the daemon. Then, restart the daemon with the appropriate privilege level.

```
# pkill in.iked
# /usr/lib/inet/in.iked -p 2
Setting privilege level to 2!
```

4. Generate random numbers and construct a key of 64 to 448 bits.

For details, see [“How to Generate Random Numbers on a Solaris System”](#) on page 460.

5. By some means, send the key to the administrator of the remote system.

You both need to add the same preshared key at the same time. Your key is only as safe as the safety of your transmission mechanism. An out-of-band mechanism, such as registered mail or a protected fax machine, is best.

6. Add the new keying material with the `add preshared` subcommand in `ikeadm` command mode.

```
ikeadm> add preshared { localidtype id-type localid id
remoteidtype id-type remoteid id ike_mode mode key key }
```

id-type Specifies the type of the *id*.

id Specifies the IP address when *id-type* is IP.

mode Specifies the IKE mode. The only accepted value is `main`.

key Specifies the preshared key in hexadecimal format.

a. For example, on host `enigma`, you would add the key for the remote system, `ada`, and exit the `ikeadm` interactive mode.

```
# ikeadm
ikeadm> add preshared { localidtype ip localid 192.168.116.16
remoteidtype ip remoteid 192.168.15.7
ike_mode main
key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d }
ikeadm: Successfully created new preshared key.
ikeadm> exit
#
```

b. On host `ada`, you would add the identical key for the remote system, `enigma`, and exit the interactive mode.

```
# ikeadm
ikeadm> add preshared { localidtype ip localid 192.168.15.7
remoteidtype ip remoteid 192.168.116.16
ike_mode main
key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d }
ikeadm: Successfully created new preshared key.
ikeadm> exit
#
```

7. On each system, lower the privilege level of the `in.iked` daemon.

```
# ikeadm set priv base
```

8. On each system, activate the `ipsecinit.conf` file to secure the added interface.

```
# ipsecconf -a /etc/inet/ipsecinit.conf
```



Caution – Read the warning when you execute the `ipsecconf` command. The same warning applies to restarting the `in.iked` daemon. A socket that is already latched, that is, the socket is in use, provides an unsecured back door into the system. For more extensive discussion, see [“Security Considerations for `ipsecinit.conf` and `ipsecconf`” on page 471.](#)

9. On each system, read in the new rules by using the `ikeadm` command.

```
# ikeadm read rules
```

You created the rules in [Step 2](#). Because the rules are in the `/etc/inet/ike/config` file, the name of the file does not have to be specified to the `ikeadm` command.

10. Ensure that IKE preshared keys are available at reboot.

Add the keys to the `/etc/inet/secret/ike.preshared` file.

a. For example, on the enigma system, you would add the following keying information to the `ike.preshared` file:

```
# ike.preshared on enigma for the ada interface
#...
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.15.7
  # enigma and ada's shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

b. On the ada system, you would add the following keying information to the `ike.preshared` file:

```
# ike.preshared on ada for the enigma interface
#...
{ localidtype IP
  localid 192.168.15.7
  remoteidtype IP
  remoteid 192.168.116.16
  # ada and enigma's shared key in hex (32 - 448 bits required)
  key 8d1fb4ee500e2bea071deb2e781cb48374411af5a9671714672bb1749ad9364d
}
```

11. Verify that the systems can communicate.

See [“How to Verify That IKE Preshared Keys Are Identical”](#) on page 494.

▼ How to Verify That IKE Preshared Keys Are Identical

If the preshared keys on the communicating systems are not identical, the systems cannot authenticate.

Before You Begin

IPsec has been configured and is enabled between the two systems that you are testing.

- Steps** 1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Check the privilege level of the `in.iked` daemon.**

```
# /usr/sbin/ikeadm get priv
Current privilege level is 0x0, base privileges enabled
```

- **If the privilege level is `0x1` or `0x2`, continue with the next step.**
- **If the privilege level is `0x0`, stop the daemon. Then, restart the daemon with the appropriate privilege level.**

```
# pkill in.iked
# /usr/lib/inet/in.iked -p 2
Setting privilege level to 2!
```

3. **On each system, view the preshared key information.**

```
# ikeadm dump preshared
PSKEY: Preshared key (24 bytes): f47cb.../192
LOCIP: AF_INET: port 0, 192.168.116.16 (enigma).
REMIP: AF_INET: port 0, 192.168.13.213 (partym).
```

4. **Compare the two dumps.**

If the preshared keys are not identical, replace one key with the other key in the `/etc/inet/secret/ike.preshared` file.

5. **When the verification is complete, lower the privilege level of the `in.iked` daemon on each system.**

```
# ikeadm set priv base
```

Configuring IKE With Public Key Certificates (Task Map)

The following table provides pointers to procedures for creating public key certificates for IKE. The procedures include how to accelerate and store the certificates on attached hardware.

Task	Description	For Instructions
Configure IKE with self-signed public key certificates	Creates and places two certificates on each system: <ul style="list-style-type: none">■ A self-signed certificate■ The public key certificate from the remote system	“How to Configure IKE With Self-Signed Public Key Certificates” on page 497
Configure IKE with a PKI Certificate Authority	Creates a certificate request, and then places three certificates on each system: <ul style="list-style-type: none">■ The certificate that the Certificate Authority (CA) creates from your request■ The public key certificate from the CA■ The CRL from the CA	“How to Configure IKE With Certificates Signed by a CA” on page 501
Configure public key certificates on local hardware	Involves one of: <ul style="list-style-type: none">■ Generating a self-signed certificate on the local hardware and then adding the public key from a remote system to the hardware.■ Generating a certificate request on the local hardware and then adding the public key certificates from the CA to the hardware.	“How to Generate and Store Public Key Certificates on Hardware” on page 506
Update the certificate revocation list (CRL) from a PKI	Accesses the CRL from a central distribution point.	“How to Handle a Certificate Revocation List” on page 510

Configuring IKE With Public Key Certificates

Public key certificates eliminate the need for communicating systems to share secret keying material out of band. Unlike preshared keys, a public key certificate can be used on a mobile machine or on a system that might be renumbered.

Public key certificates can also be stored on attached hardware. For the procedure, see “Configuring IKE to Find Attached Hardware (Task Map)” on page 520.

▼ How to Configure IKE With Self-Signed Public Key Certificates

Self-signed certificates require less overhead than public certificates from a CA, but do not scale very easily.

- Steps**
1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Add a self-signed certificate to the `ike.privatekeys` database.**

```
# ikecert certlocal -ks|-kc -m keysize -t keytype \  
-D dname -A altname
```

- | | |
|-------------------|---|
| -ks | Creates a self-signed certificate. |
| -kc | Creates a certificate request. For the procedure, see “How to Configure IKE With Certificates Signed by a CA” on page 501. |
| -m <i>keysize</i> | Is the size of the key. The <i>keysize</i> can be 512, 1024, 2048, 3072, or 4096. |
| -t <i>keytype</i> | Specifies the type of algorithm to use. The <i>keytype</i> can be <code>rsa-sha1</code> , <code>rsa-md5</code> , or <code>dsa-sha1</code> . |
| -D <i>dname</i> | Is the X.509 distinguished name for the certificate subject. The <i>dname</i> typically has the form: C=country, O=organization, OU=organizational unit, CN=common name. Valid tags are C, O, OU, and CN. |
| -A <i>altname</i> | Is the alternate name for the certificate. The <i>altname</i> is in the form of <code>tag=value</code> . Valid tags are IP, DNS, EMAIL, and DN. |

- a. **For example, the command on the `partym` system would appear similar to the following:**

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \  
-D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \  

```

```

-A IP=192.168.13.213
Creating software private keys.
  Writing private key to file /etc/inet/secret/ike.privatekeys/0.
Enabling external key providers - done.
Acquiring private keys for signing - done.
Certificate:
  Proceeding with the signing operation.
  Certificate generated successfully (.../publickeys/0)
Finished successfully.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICLTCCAzagAwIBAgIBATANBgkqhkiG9w0BAQQFADBNMQswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----

```

b. The command on the enigma system would appear similar to the following:

```

# ikecert certlocal -ks -m 1024 -t rsa-md5 \
-D "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax" \
-A IP=192.168.116.16
Creating software private keys.
...
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIICKDCCAzGgAwIBAgIBATANBgkqhkiG9w0BAQQFADBJMQswCQYDVQQGEwJVUzEV
...
jpxfLM98xyFVyLChkr3dZ3Tvxvi732BXePKF2A==
-----END X509 CERTIFICATE-----

```

3. Save the certificate and send it to the remote system.

You can paste the certificate into an email.

a. For example, you would send the following partym certificate to the enigma administrator:

```

To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICLTCCAzagAwIBAgIBATANBgkqhkiG9w0BAQQFADBNMQswCQYDVQQGEwJVUzEX
...
6sKTxpg4GP3GkQGcd0r1rhW/3yaWBkDwOdFCqEUyffzU
-----END X509 CERTIFICATE-----

```

b. The enigma administrator would send you the following enigma certificate:

```

To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIICKDCCAzGgAwIBAgIBATANBgkqhkiG9w0BAQQFADBJMQswCQYDVQQGEwJVUzEV
...
jpxfLM98xyFVyLChkr3dZ3Tvxvi732BXePKF2A==
-----END X509 CERTIFICATE-----

```

4. On each system, trust both certificates.

Edit the `/etc/inet/ike/config` file to recognize the certificates.

The administrator of the remote system provides the values for the `cert_trust`, `remote_addr`, and `remote_id` parameters.

a. For example, on the `partym` system, the `ike/config` file would appear similar to the following:

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

cert_trust "192.168.13.213"
cert_trust "192.168.116.16"

## Parameters that may also show up in rules.

p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg des }
p2_pfs 5

{
  label "US-partym to JA-enigmax"
  local_id_type dn
  local_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
  remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

  local_addr 192.168.13.213
  remote_addr 192.168.116.16

  p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg md5 encr_alg 3des}
}
```

b. On the `enigma` system, add `enigma` values for local parameters in the `ike/config` file.

For the remote parameters, use `partym` values. Ensure that the value for the `label` keyword is unique. This value must be different from the remote system's `label` value.

```
...
{
  label "JA-enigmax to US-partym"
  local_id_type dn
  local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
  remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  ...
}
```

5. On each system, add the certificate that you received.

- a. Copy the public key from the administrator's email.
- b. Type the `ikecert certdb -a` command and press the Return key.
No prompts display when you press the Return key.
- c. Paste the public key. Then press the Return key. To end the entry, press Control-D.

```
# ikecert certdb -a      Press the Return key

-----BEGIN X509 CERTIFICATE-----
MIIC...
...
-----END X509 CERTIFICATE-----      Press the Return key
<Control>-D
```

6. List the stored certificate on your system.

For example, on the `partym` system, the public certificate is in slot 1, and the private certificate is in slot 0.

```
partym # ikecert certdb -l
Certificate Slot Name: 0      Type: rsa-md5      Private Key
  Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
  Key Size: 1024
  Public key hash: B2BD13FCE95FD27ECE6D2DCD0DE760E2

Certificate Slot Name: 1      Type: rsa-md5      Public Certificate
  (Private key in certlocal slot 0)      Points to certificate's private key
  Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
  Key Size: 1024
  Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

7. Verify with the other administrator that the keys have not been tampered with.

For example, you can phone the other administrator to compare the values of the public key hash. The public key hash for the shared certificate should be identical on the two systems.

Compare this value with the public key hash on the `enigma` system:

```
enigma # ikecert certdb -l
Certificate Slot Name: 4      Type: rsa-md5      Private Key
  Subject Name: <C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax>
  Key Size: 1024
  Public key hash: DF3F108F6AC669C88C6BD026B0FCE3A0

Certificate Slot Name: 5      Type: rsa-md5      Public Certificate
  (Private key in certlocal slot 4)
  Subject Name: <C=US, O=PartyCompany, OU=US-Partym, CN=Partym>
  Key Size: 1024
  Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

Note – In this example, the public key hash is different from the public key hash that your systems generate.

▼ How to Configure IKE With Certificates Signed by a CA

Public certificates from a Certificate Authority (CA) require negotiation with an outside organization. The certificates very easily scale to protect a large number of communicating systems.

- Steps**
1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Use the `ikecert certlocal -kc` command to create a certificate request.**

For a description of the arguments to the command, see Step 2 in “How to Configure IKE With Self-Signed Public Key Certificates” on page 497.

```
# ikecert certlocal -kc -m keysize -t keytype \  
-D dname -A altname
```

- a. **For example, the following command creates a certificate request on the `partym` system:**

```
# ikecert certlocal -kc -m 1024 -t rsa-md5 \  
> -D "C=US, O=PartyCompany\, Inc., OU=US-Partym, CN=Partym" \  
> -A "DN=C=US, O=PartyCompany\, Inc., OU=US-Partym"  
Creating software private keys.  
Writing private key to file /etc/inet/secret/ike.privatekeys/2.  
Enabling external key providers - done.  
Certificate Request:  
Proceeding with the signing operation.  
Certificate request generated successfully (.../publickeys/0)  
Finished successfully.  
-----BEGIN CERTIFICATE REQUEST-----
```

```

MIIBYjCCATMCAQAwUzELMAkGA1UEBhMCVVMxHTAbBgNVBAoTFEV4YW1wbGVDb21w
...
lcM+tw0ThRrfuJX9t/Qa1R/KxRlMA3zckO80mO9X
-----END CERTIFICATE REQUEST-----

```

b. The following command creates a certificate request on the enigma system:

```

# ikecert certlocal -kc -m 1024 -t rsa-md5 \
> -D "C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax, CN=Enigmax" \
> -A "DN=C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax"
Creating software private keys.
...
Finished successfully.
-----BEGIN CERTIFICATE REQUEST-----
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu
...
8qlqджаStLGfhDOO
-----END CERTIFICATE REQUEST-----

```

3. Submit the certificate request to a PKI organization.

The PKI organization can tell you how to submit the certificate request. Most organizations have a web site with a submission form. The form requires proof that the submission is legitimate. Typically, you paste your certificate request into the form. When your request has been checked by the organization, the organization issues you the following two certificate objects and a list of revoked certificates:

- Your public key certificate – This certificate is based on the request that you submitted to the organization. The request that you submitted is part of this public key certificate. The certificate uniquely identifies you.
- A Certificate Authority – The organization’s signature. The CA verifies that your public key certificate is legitimate.
- A Certificate Revocation List (CRL) – The latest list of certificates that the organization has revoked. The CRL is not sent separately as a certificate object if access to the CRL is embedded in the public key certificate.

When a URI for the CRL is embedded in the public key certificate, IKE can automatically retrieve the CRL for you. Similarly, when a DN (directory name on an LDAP server) entry is embedded in the public key certificate, IKE can retrieve and cache the CRL from an LDAP server that you specify.

See [“How to Handle a Certificate Revocation List” on page 510](#) for an example of an embedded URI and an embedded DN entry in a public key certificate.

4. Add each certificate to your system.

The `-a` option to the `ikecert certdb -a` adds the pasted object to the appropriate certificate database on your system. For more information, see [“IKE With Public Key Certificates” on page 480](#).

- a. On the system console, assume the Primary Administrator role or become superuser.**

- b. Add the public key certificate that you received from the PKI organization.

```
# ikecert certdb -a
  Press the Return key
  Paste the certificate:
-----BEGIN X509 CERTIFICATE-----
...
-----END X509 CERTIFICATE-----
  Press the Return key
<Control>-D
```

- c. Add the CA from the PKI organization.

```
# ikecert certdb -a
  Press the Return key
  Paste the CA:
-----BEGIN X509 CERTIFICATE-----
...
-----END X509 CERTIFICATE-----
  Press the Return key
<Control>-D
```

- d. If the PKI organization has sent a list of revoked certificates, add the CRL to the `certrldb` database:

```
# ikecert certrldb -a
  Press the Return key
  Paste the CRL:
-----BEGIN CRL-----
...
-----END CRL-----
  Press the Return key
<Control>-D
```

5. Use the `cert_root` keyword to identify the PKI organization in the `/etc/inet/ike/config` file.

Use the name that the PKI organization provides.

- a. For example, the `ike/config` file on the `partym` system might appear similar to the following:

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

## Parameters that may also show up in rules.

p1_xform
{ auth_method rsa_sig oakley_group 1 auth_alg sha1 encr_alg des }
p2_pfs 2

{
```

```

label "US-party to JA-enigmax - Example PKI"
local_id_type dn
local_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

local_addr 192.168.13.213
remote_addr 192.168.116.16

p1_xform
{auth_method rsa_sig oakley_group 2 auth_alg md5 encr_alg 3des}
}

```

Note – All arguments to the `auth_method` parameter must be on the same line.

b. On the enigma system, create a similar file.

Specifically, the enigma `ike/config` file should do the following:

- Include the same `cert_root` value.
- Use enigma values for local parameters.
- Use party values for remote parameters.
- Create a unique value for the `label` keyword. This value must be different from the remote system's label value.

```

...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"
...
{
  label "JA-enigmax to US-party - Example PKI"
  local_id_type dn
  local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
  remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

  local_addr 192.168.116.16
  remote_addr 192.168.13.213
...

```

6. Tell IKE how to handle CRLs.

Choose the appropriate option:

- **No CRL available**

If the PKI organization does not provide a CRL, add the keyword `ignore_crls` to the `ike/config` file.

```

# Trusted root cert
...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, ...
ignore_crls
...

```


The `ignore_crls` keyword tells IKE not to search for CRLs.

- **CRL available**

If the PKI organization provides a central distribution point for CRLs, you can modify the `ike/config` file to point to that location.

See “How to Handle a Certificate Revocation List” on page 510 for examples.

Example 22-1 Using `rsa_encrypt` When Configuring IKE

When you use `auth_method rsa_encrypt` in the `ike/config` file, you must add the peer’s certificate to the `publickeys` database.

1. Send the certificate to the remote system’s administrator.

You can paste the certificate into an email.

For example, the `partym` administrator would send the following email:

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MII...
-----END X509 CERTIFICATE-----
```

The `enigma` administrator would send the following email:

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MII
...
-----END X509 CERTIFICATE-----
```

2. On each system, add the emailed certificate to the local `publickeys` database.

```
# ikecert certdb -a
  Press the Return key
-----BEGIN X509 CERTIFICATE-----
MII...
-----END X509 CERTIFICATE-----
  Press the Return key
<Control>-D
```

The authentication method for RSA encryption hides identities in IKE from eavesdroppers. Because the `rsa_encrypt` method hides the peer’s identity, IKE cannot retrieve the peer’s certificate. As a result, the `rsa_encrypt` method requires that the IKE peers know each other’s public keys.

Therefore, when you use an `auth_method` of `rsa_encrypt` in the `/etc/inet/ike/config` file, you must add the peer’s certificate to the `publickeys` database. The `publickeys` database then holds three certificates for each communicating pair of systems:

- Your public key certificate
- The CA certificate
- The peer's public key certificate

Troubleshooting – The IKE payload, which includes the three certificates, can become too large for `rsa_encrypt` to encrypt. Errors such as “authorization failed” and “malformed payload” can indicate that the `rsa_encrypt` method cannot encrypt the total payload. Reduce the size of the payload by using a method, such as `rsa_sig`, that requires only two certificates.

▼ How to Generate and Store Public Key Certificates on Hardware

Generating and storing public key certificates on hardware is similar to generating and storing public key certificates on your system. There are two differences:

- The `ikecert certlocal` and `ikecert certdb` commands must identify the hardware. The `-T` option with the token ID identifies the hardware to the commands.
- The `/etc/inet/ike/config` file must point to the hardware with the `pkcs11_path` keyword.
- The hardware must be configured.
- The `/etc/inet/ike/config` file must point to a library that is implemented according to the following standard: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki), that is, a PKCS #11 library.

Before You Begin

See “[How to Configure IKE to Find the Sun Crypto Accelerator 4000 Board](#)” on page 522 for setup instructions.

- Steps**
1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Generate a self-signed certificate or a certificate request, and specify the token ID.**

Choose one of the following options:

Note – The Sun Crypto Accelerator 4000 board supports keys up to 2048 bits for RSA. For DSA, this board supports keys up to 1024 bits.

■ **For a self-signed certificate, use this syntax.**

```
# ikecert certlocal -ks -m 1024 -t rsa-md5 \  
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \  
> -a -T dca0-accel-stor IP=192.168.116.16  
Creating hardware private keys.  
Enter PIN for PKCS#11 token:      Type user:password
```

The argument to the `-T` option is the token ID from the attached Sun Crypto Accelerator 4000 board.

■ **For a certificate request, use this syntax.**

```
# ikecert certlocal -kc -m 1024 -t rsa-md5 \  
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \  
> -a -T dca0-accel-stor IP=192.168.116.16  
Creating hardware private keys.  
Enter PIN for PKCS#11 token:      Type user:password
```

For a description of the arguments to the `ikecert` command, see the `ikecert(1M)` man page.

3. **At the prompt for a PIN, type the Sun Crypto Accelerator 4000 user, a colon, and the user's password.**

If the Sun Crypto Accelerator 4000 board has a user `ikemgr` whose password is `rgm4tigt`, you would type the following:

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt
```

Note – The PIN response is stored on disk *as clear text*.

After you type the password, the certificate prints out:

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt  
-----BEGIN X509 CERTIFICATE-----  
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu  
...  
oKUDBbZ9O/pLWYGr  
-----END X509 CERTIFICATE-----
```

4. **Send your certificate for use by the other party.**

Choose one of the following options:

- **Send the self-signed certificate to the remote system.**

You can paste the certificate into an email.

- **Send the certificate request to an organization that handles PKI.**

Follow the instructions of the PKI organization to submit the certificate request. For a more detailed discussion, see [Step 3](#) of “How to Configure IKE With Certificates Signed by a CA” on page 501.

5. On your system, edit the `/etc/inet/ike/config` file to recognize the certificates.

Choose one of the following options.

- **Self-signed certificate**

Use the values that the administrator of the remote system provides for the `cert_trust`, `remote_id`, and `remote_addr` parameters. For example, on the `enigma` system, the `ike/config` file would appear similar to the following:

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

cert_trust "192.168.116.16"      Local system's certificate
cert_trust "192.168.13.213"    Remote system's certificate

pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"  Hardware
connection

...
{
  label "JA-enigmax to US-partym"
  local_id_type dn
  local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
  remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

  local_addr 192.168.116.16
  remote_addr 192.168.13.213

  p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg md5 encr_alg 3des}
}
```

- **Certificate request**

Type the name that the PKI organization provides as the value for the `cert_root` keyword. For example, the `ike/config` file on the `enigma` system might appear similar to the following:

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"
```

```
pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
...
{
  label "JA-enigmax to US-partym - Example PKI"
  local_id_type dn
  local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
  remote_id "C=US, O=PartyCompany, OU=US-Party, CN=Party"

  local_addr 192.168.116.16
  remote_addr 192.168.13.213

  p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg md5 encr_alg 3des}
}
```

Hardware connection

6. Place the certificates from the other party in the hardware.

Respond to the PIN request as you responded in [Step 3](#).

Note – You *must* add the public key certificates to the same attached hardware that generated your private key.

■ **Self-signed certificate.**

Add the remote system’s self-signed certificate.

```
# ikecert certdb -a -T dca0-accel-stor
```

Press the Return key

Paste the self-signed certificate

```
<Control>-D
```

Enter PIN for PKCS#11 token: *Type user:password*

If the self-signed certificate used `rsa_encrypt` as the value for the `auth_method` parameter, add the peer’s certificate to the hardware store.

■ **Certificates from a PKI organization.**

Add the certificate that the organization generated from your certificate request, and add the certificate authority (CA).

```
# ikecert certdb -a -T dca0-accel-stor
```

Press the Return key

Paste the returned certificate

```
<Control>-D
```

Enter PIN for PKCS#11 token: *Type user:password*

```
# ikecert certdb -a -T dca0-accel-stor
```

Press the Return key

Paste the CA certificate

```
<Control>-D
```

Enter PIN for PKCS#11 token: *Type user:password*

To add a certificate revocation list (CRL) from the PKI organization, see [“How to Handle a Certificate Revocation List”](#) on page 510.

▼ How to Handle a Certificate Revocation List

A certificate revocation list (CRL) contains outdated or compromised certificates from a Certificate Authority. You have four ways to handle CRLs.

- You must instruct IKE to ignore CRLs if your CA organization does not issue CRLs. This option is shown in [Step 6](#) in [“How to Configure IKE With Certificates Signed by a CA”](#) on page 501.
- You can instruct IKE to access the CRLs from a URI (uniform resource indicator) whose address is embedded in the public key certificate from the CA.
- You can instruct IKE to access the CRLs from an LDAP server whose DN (directory name) entry is embedded in the public key certificate from the CA.
- You can provide the CRL as an argument to the `ikecert certrladb` command. For an example, see [Example 22-2](#).

The following procedure describes how to instruct IKE to use CRLs from a central distribution point.

Steps 1. Display the certificate that you received from the CA.

```
# ikecert certdb -lv certspec
-l          Lists certificates in the IKE certificate database.
-v          Lists the certificates in verbose mode. Use this option with care.

certspec  Is a pattern that matches a certificate in the IKE certificate database.
For example, the following certificate was issued by Sun Microsystems. Details
have been altered.

# ikecert certdb -lv example-protect.sun.com
Certificate Slot Name: 0   Type: dsa-sha1
  (Private key in certlocal slot 0)
Subject Name: <O=Sun Microsystems Inc, CN=example-protect.sun.com>
Issuer Name: <CN=Sun Microsystems Inc CA (C1 B), O=Sun Microsystems Inc>
SerialNumber: 14000D93
Validity:
  Not Valid Before: 2002 Jul 19th, 21:11:11 GMT
  Not Valid After:  2005 Jul 18th, 21:11:11 GMT
Public Key Info:
  Public Modulus (n) (2048 bits): C575A...A5
  Public Exponent (e) ( 24 bits): 010001
Extensions:
  Subject Alternative Names:
    DNS = example-protect.sun.com
```

```

Key Usage: DigitalSignature KeyEncipherment
[CRITICAL]
CRL Distribution Points:
Full Name:
  URI = #Ihttp://www.sun.com/pki/pkismica.crl#i
  DN = <CN=Sun Microsystems Inc CA (C1 B), O=Sun Microsystems Inc>
CRL Issuer:
Authority Key ID:
Key ID:          4F ... 6B
SubjectKeyID:    A5 ... FD
Certificate Policies
Authority Information Access

```

Notice the CRL Distribution Points entry. The URI entry indicates that this organization's CRL is available on the web. The DN entry indicates that the CRL is available on an LDAP server. Once accessed by IKE, the CRL is cached for further use.

To access the CRL, you need to reach a distribution point.

2. Choose one of the following methods to access the CRL from a central distribution point.

- **Use the URI.**

Add the keyword `use_http` to the host's `/etc/inet/ike/config` file. For example, the `ike/config` file would appear similar to the following:

```

# Use CRL from organization's URI
use_http
...

```

- **Use a web proxy.**

Add the keyword `proxy` to the `ike/config` file. The `proxy` keyword takes a URL as an argument, as in the following:

```

# Use own web proxy
proxy "http://proxy1:8080"

```

- **Use an LDAP server.**

Name the LDAP server as an argument to the `ldap-list` keyword in the host's `/etc/inet/ike/config` file. Your organization provides the name of the LDAP server. The entry in the `ike/config` file would appear similar to the following:

```

# Use CRL from organization's LDAP
ldap-list "ldap1.sun.com:389,ldap2.sun.com"
...

```

IKE retrieves the CRL and caches the CRL until the certificate expires.

Example 22-2 Pasting a CRL Into the Local `cert1db` Database

If the PKI organization's CRL is not available from a central distribution point, you can add the CRL manually to the local `cert1db` database. Follow the PKI organization's instructions for extracting the CRL, then add the CRL to the database with the `ikecert cert1db -a` command.

```
# ikecert cert1db -a  
    Press the Return key  
    Paste the CRL from the PKI organization  
    Press the Return key  
    Press <Control>-D to enter the CRL into the database
```

Configuring IKE for Mobile Systems (Task Map)

The following table points to procedures to configure IKE to handle systems that log in remotely to a central site.

Task	Description	For Instructions
Communicate with a central site from off-site	Enables off-site systems to communicate with a central site. The off-site systems might be mobile.	"How to Configure IKE for Off-Site Systems" on page 513
Use a root certificate and IKE on a central system that accepts traffic from mobile systems	Configures a gateway system to accept IPsec traffic from a system that does not have a fixed IP address.	Example 22-3
Use a root certificate and IKE on a system that does not have a fixed IP address	Configures a mobile system to protect its traffic to a central site, such as company headquarters.	Example 22-4
Use self-signed certificates and IKE on a central system that accepts traffic from mobile systems	Configures a gateway system with self-signed certificates to accept IPsec traffic from a mobile system.	Example 22-5
Use self-signed certificates and IKE on a system that does not have a fixed IP address	Configures a mobile system with self-signed certificates to protect its traffic to a central site.	Example 22-6

Configuring IKE for Mobile Systems

When configured properly, home offices and mobile laptops can use IPsec and IKE to communicate with their company's central computers. A blanket IPsec policy that is combined with a public key authentication method enables off-site systems to protect their traffic to a central system.

▼ How to Configure IKE for Off-Site Systems

IPsec and IKE require a unique ID to identify source and destination. For off-site or mobile systems that do not have a unique IP address, you must use another ID type. ID types such as DNS, DN, or EMAIL can be used to uniquely identify a system.

Off-site or mobile systems that have unique IP addresses are still best configured with a different ID type. For example, if the systems attempt to connect to a central site from behind a NAT box, their unique addresses are not used. A NAT box assigns an arbitrary IP address, which the central system would not recognize.

Preshared keys also do not work well as an authentication mechanism for mobile systems, because preshared keys require fixed IP addresses. Self-signed certificates, or certificates from a PKI enable mobile systems to communicate with the central site.

- Steps**
1. **On the system console of the central system, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, "Working With the Solaris Management Console (Tasks)," in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Configure the central system to recognize mobile systems.**

- a. **Set up the `/etc/hosts` file.**

The central system does not have to recognize specific addresses for the mobile systems.

```
# /etc/hosts on central
central 192.xxx.xxx.x
```

b. Set up the `ipsecinit.conf` file.

The central system needs a policy that allows a wide range of IP addresses. Later, certificates in the IKE policy ensure that the connecting systems are legitimate.

```
# /etc/inet/ipsecinit.conf on central
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs md5 sa shared}
```

c. Set up the `ike.config` file.

DNS identifies the central system. Certificates are used to authenticate the system.

```
# /etc/inet/ike/ike.config on central
# Global parameters
# Enable faster public key operations
pkcs11_path "/usr/lib/libpkcs11.so"
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server "ldap-server1.domain.org, ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root "C=US, O=Domain Org, CN=Domain STATE"
#
# List self-signed certificates - trust server and enumerated others
#cert_trust "DNS=central.domain.org"
#cert_trust "DNS=mobile.domain.org"
#cert_trust "DN=CN=Domain Org STATE (CLASS), O=Domain Org"
#cert_trust "EMAIL=root@central.domain.org"
#cert_trust "EMAIL=user1@mobile.domain.org"
#
# Rule for mobile systems with certificate
{
  label "Mobile systems with certificate"
  local_id_type DNS
}
# Any mobile system who knows my DNS or IP can find me.
local_id "central.domain.org"
local_addr 192.xxx.xxx.x
# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
remote_id ""
remote_addr 0.0.0.0/0
```

```

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg md5 }
}

```

3. Log in to each mobile system, and configure the system to find the central system.

a. Set up the `/etc/hosts` file.

The `/etc/hosts` file does not need an address for the mobile system, but can provide one. The file must contain a public IP address for the central system.

```

# /etc/hosts on mobile
mobile 10.x.x.x
central 192.xxx.xxx.x

```

b. Set up the `ipsecinit.conf` file.

The mobile system needs to find the central system by its public IP address. The systems must configure the same IPsec policy.

```

# /etc/inet/ipsecinit.conf on mobile
# Find central
{raddr 192.xxx.xxx.x} ipsec {encr_algs aes encr_auth_algs md5 sa shared}

```

c. Set up the `ike.config` file.

The identifier cannot be an IP address. The following identifiers are valid for mobile systems:

- `DN=ldap-directory-name`
- `DNS=domain-name-server-address`
- `EMAIL=email-address`

Certificates are used to authenticate the mobile system.

```

# /etc/inet/ike/ike.config on mobile
# Global parameters
# Enable faster public key operations
pkcs11_path "/usr/lib/libpkcs11.so"
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root "C=US, O=Domain Org, CN=Domain STATE"
#
# Self-signed certificates - trust me and enumerated others

```

```

#cert_trust      "DNS=mobile.domain.org"
#cert_trust      "DNS=central.domain.org"
#cert_trust      "DN=CN=Domain Org STATE (CLASS), O=Domain Org"
#cert_trust      "EMAIL=user1@domain.org"
#cert_trust      "EMAIL=root@central.domain.org"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile with certificate"
    local_id_type DNS

# NAT-T can translate local_addr into any public IP address
# central knows me by my DNS

    local_id "mobile.domain.org"
    local_addr 0.0.0.0/0

# Find central and trust the root certificate
    remote_id "central.domain.org"
    remote_addr 192.xxx.xxx.x

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg md5 }
}

```

4. Reboot each system when it is configured.

Or, stop and start the `in.iked` daemon.

Example 22-3 Configuring a Central Computer to Accept IPsec Traffic From a Mobile System

IKE can initiate negotiations from behind a NAT box. However, the ideal setup for IKE is without an intervening NAT box. In the following example, root certificates have been issued by a CA. The CA certificates have been placed on the mobile and the central system. A central system accepts IPsec negotiations from a system behind a NAT box. `main1` is the company system that can accept connections from off-site systems. To set up the off-site systems, see [Example 22-4](#).

```

# /etc/hosts on main1
main1 192.168.0.100

# /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs md5 sa shared}

# /etc/inet/ike/ike.config on main1
# Global parameters
# Enable faster public key operations
pkcs11_path "/usr/lib/libpkcs11.so"
#
#

```

```

# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server "ldap1.domain.org,ldap2.domain.org:389"
#
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
  label "Off-site system with root certificate"
  local_id_type DNS
  local_id "main1.domain.org"
  local_addr 192.168.0.100

# Root certificate ensures trust,
# so allow any remote_id and any remote IP address.
  remote_id ""
  remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg md5}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg 3des auth_alg md5}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg sha}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg 3des auth_alg sha}
}

```

Example 22-4 Configuring a System Behind a NAT With IPsec

In the following example, root certificates have been issued by a CA and placed on the mobile and the central system. `mobile1` is connecting to the company headquarters from home. The Internet service provider (ISP) network uses a NAT box to enable the ISP to assign `mobile1` a private address. The NAT box then translates the private address into a public IP address that is shared with other ISP network nodes. Company headquarters is not behind a NAT. For setting up the computer at company headquarters, see [Example 22-3](#).

```

# /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

# /etc/inet/ipsecinit.conf on mobile1
# Find main1

```

```

{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs md5 sa shared}

# /etc/inet/ike/ike.config on mobile1
# Global parameters
# Enable faster public key operations
pkcs11_path "/usr/lib/libpkcs11.so"
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile1 with root certificate"
    local_id_type DNS
    local_id "mobile1.domain.org"
    local_addr 0.0.0.0/0

# Find main1 and trust the root certificate
remote_id "main1.domain.org"
remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg md5 }
}

```

Example 22-5 Accepting Self-Signed Certificates From a Mobile System

In the following example, self-signed certificates have been issued and are on the mobile and the central system. `main1` is the company system that can accept connections from off-site systems. To set up the off-site systems, see [Example 22-6](#).

```

# /etc/hosts on main1
main1 192.168.0.100

# /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs md5 sa shared}

# /etc/inet/ike/ike.config on main1
# Global parameters
#
# Self-signed certificates - trust me and enumerated others
cert_trust "DNS=main1.domain.org"

```

```

cert_trust    "jdoe@domain.org"
cert_trust    "user2@domain.org"
cert_trust    "user3@domain.org"
#
# Rule for off-site systems with trusted certificate
{
    label "Off-site systems with trusted certificates"
    local_id_type DNS
    local_id "main1.domain.org"
    local_addr 192.168.0.100

# Trust the self-signed certificates
# so allow any remote_id and any remote IP address.
    remote_id ""
    remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg md5 }
}

```

Example 22-6 Using Self-Signed Certificates to Contact a Central System

In the following example, `mobile1` is connecting to the company headquarters from home. The certificates have been issued and placed on the mobile and the central system. The ISP network uses a NAT box to enable the ISP to assign `mobile1` a private address. The NAT box then translates the private address into a public IP address that is shared with other ISP network nodes. Company headquarters is not behind a NAT. To set up the computer at company headquarters, see [Example 22-5](#).

```

# /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

# /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs md5 sa shared}

# /etc/inet/ike/ike.config on mobile1
# Global parameters

# Self-signed certificates - trust me and the central system
cert_trust    "jdoe@domain.org"
cert_trust    "DNS=main1.domain.org"
#
# Rule for off-site systems with trusted certificate
{
    label "Off-site mobile1 with trusted certificate"
    local_id_type EMAIL
    local_id "jdoe@domain.org"
    local_addr 0.0.0.0/0

# Find main1 and trust the certificate

```

```

remote_id "main1.domain.org"
remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg blowfish auth_alg md5 }
}

```

Configuring IKE to Find Attached Hardware (Task Map)

The following table points to procedures that inform IKE about attached hardware. You must inform IKE about attached hardware before IKE can use the hardware. To use the hardware, follow the hardware procedures in [“Configuring IKE With Public Key Certificates” on page 496](#).

Task	Description	For Instructions
Offload IKE key operations to the Sun Crypto Accelerator 1000 board	Links IKE to the PKCS#11 library.	“How to Configure IKE to Find the Sun Crypto Accelerator 1000 Board” on page 521
Offload IKE key operations and store the keys on the Sun Crypto Accelerator 4000 board	Links IKE to the PKCS#11 library and lists the name of the attached hardware.	“How to Configure IKE to Find the Sun Crypto Accelerator 4000 Board” on page 522

Configuring IKE to Find Attached Hardware

Public key certificates can also be stored on attached hardware, the Sun Crypto Accelerator 1000 board and the Sun Crypto Accelerator 4000 board. With the Sun Crypto Accelerator 4000 board, public key operations can also be offloaded from the system to the board.

▼ How to Configure IKE to Find the Sun Crypto Accelerator 1000 Board

Before You Begin

The following procedure assumes that a Sun Crypto Accelerator 1000 board is attached to the system. The procedure also assumes that the software for the board has been installed and that the software has been configured. For instructions, see the *Sun Crypto Accelerator 1000 Board Version 1.1 Installation and User's Guide*.

Steps 1. On the system console, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, "Working With the Solaris Management Console (Tasks)," in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. Add the PKCS #11 library path to the `/etc/inet/ike/config` file.

```
pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

The path name must point to a 32-bit PKCS #11 library. If the library is present, IKE uses the library's routines to accelerate IKE public key operations on the Sun Crypto Accelerator 1000 board. When the board handles these expensive operations, operating system resources are free for other operations.

3. Close the file and reboot.

4. After rebooting, check that the library has been linked.

Type the following command to determine whether a PKCS #11 library has been linked:

```
# ikeadm get stats
Phase 1 SA counts:
Current:  initiator:          0  responder:          0
Total:    initiator:          0  responder:          0
Attempted: initiator:          0  responder:          0
Failed:   initiator:          0  responder:          0
          initiator fails include 0 time-out(s)
PKCS#11 library linked in from /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
#
```

Unlike other parameters in the `/etc/inet/ike/config` file, the `pkcs11_path` keyword is read only when IKE is started. If you use the `ikeadm` command to add or reload a new `/etc/inet/ike/config` file, the `pkcs11_path` persists. The path persists because the IKE daemon does not clobber data from the Phase 1

exchange. Keys that are accelerated by PKCS #11 are part of Phase 1 data.

▼ How to Configure IKE to Find the Sun Crypto Accelerator 4000 Board

Before You Begin

The following procedure assumes that a Sun Crypto Accelerator 4000 board is attached to the system. The procedure also assumes that the software for the board has been installed and that the software has been configured. For instructions, see the *Sun Crypto Accelerator 4000 Board Installation and User's Guide*. The guide is available from the <http://www.sun.com/products-n-solutions/hardware/docs> web site, under Network and Security Products.

Steps 1. On the system console, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, "Working With the Solaris Management Console (Tasks)," in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. Add the PKCS #11 library path to the `/etc/inet/ike/config` file.

```
pkcs11_path "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so"
```

The path name must point to a 32-bit PKCS #11 library. If the library is present, IKE uses the library's routines to handle key generation and key storage on the Sun Crypto Accelerator 4000 board.

3. Close the file and reboot.

4. After rebooting, check that the library has been linked. Type the following command to determine whether a PKCS #11 library has been linked:

```
$ ikeadm get stats
...
PKCS#11 library linked in from /opt/SUNWconn/cryptov2/lib/libvpkcs11.so
$
```

Unlike other parameters in the `/etc/inet/ike/config` file, the `pkcs11_path` keyword is read only when IKE is started. If you use the `ikeadm` command to add or reload a new `/etc/inet/ike/config` file, the `pkcs11_path` persists. The path persists because the IKE daemon does not clobber Phase 1 data.

Note – The Sun Crypto Accelerator 4000 board supports keys up to 2048 bits for RSA. For DSA, this board supports keys up to 1024 bits.

5. Find the token ID for the attached Sun Crypto Accelerator 4000 board.

```
$ ikecert tokens
Available tokens with library "/opt/SUNWconn/cryptov2/lib/libvpkcs11.so":

"vca0-accel                "
"dca0-accel-store         "
```

The library returns a token ID, also called a [keystore name](#), of 32 characters. In this example, you could use the `dca0-accel-store` token with the `ikecert` commands to store and to accelerate IKE keys.

For instructions on how to use the token, see [“How to Generate and Store Public Key Certificates on Hardware”](#) on page 506.

The trailing spaces are automatically padded by the `ikecert` command.

Changing IKE Transmission Parameters (Task Map)

The following table points to procedures to configure transmission parameters for IKE.

Task	Description	For Instructions
Make key negotiation more efficient	Changes the key negotiation parameters.	“How to Change the Duration of Phase 1 IKE Key Negotiation” on page 524
Configure key negotiation to allow for delays in transmission	Lengthens the key negotiation parameters.	Example 22-7
Configure key negotiation to succeed quickly, or to show failures quickly	Shortens the key negotiation parameters.	Example 22-8

Changing IKE Transmission Parameters

When IKE negotiates keys, the speed of transmission can affect the success of the negotiation. Normally, you would not need to change the default values for IKE transmission parameters. However, when optimizing key negotiation over very dirty lines, or when reproducing a problem, you might want to change the transmission values.

Longer duration times enable IKE to negotiate keys over unreliable transmission lines. You can lengthen certain parameters so that initial attempts succeed. If the initial attempt does not succeed, you can space subsequent attempts to offer more time for success.

Shorter duration times enable you to take advantage of reliable transmission lines. You can more quickly retry a failed negotiation to speed up the negotiation. When diagnosing a problem, you might also want to speed up the negotiation for a quick failure. Shorter durations also enable the Phase 1 SAs to be used for their lifetime.

▼ How to Change the Duration of Phase 1 IKE Key Negotiation

- Steps**
1. **On the system console, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

Note – Logging in remotely exposes security-critical traffic to eavesdropping. Even if you somehow protect the remote login, the security of the system is reduced to the security of the remote login session.

2. **Change the default values of the global transmission parameters on each system.**

On each system, modify Phase 1 duration parameters the `/etc/inet/ike/config` file.

```
### ike/config file on      system

## Global parameters
#
```

```

## Phase 1 transform defaults
#
#expire_timer      300
#retry_limit       5
#retry_timer_init  0.5 (integer or float)
#retry_timer_max   30  (integer or float)

expire_timer      The number of seconds to let a not-yet-complete IKE
                   Phase I negotiation linger before deleting the negotiation
                   attempt. By default, the attempt lingers for 30 seconds.

retry_limit        The number of retransmits before any IKE negotiation is
                   aborted. By default, IKE tries five times.

retry_timer_init   The initial interval between retransmits. This interval is
                   doubled until the retry_timer_max value is reached.
                   The initial interval is 0.5 seconds.

retry_timer_max    The maximum interval in seconds between retransmits.
                   The retransmit interval stops growing at this limit. By
                   default, the limit is 30 seconds.

```

3. Reboot the system.

Or, stop and start the `in.iked` daemon.

Example 22-7 Lengthening IKE Phase 1 Negotiation Times

In the following example, a system is connected to its IKE peers by a high-traffic transmission line. The original settings are in comments in the file. The new settings lengthen the negotiation time.

```

### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer      300
#retry_limit       5
#retry_timer_init  0.5 (integer or float)
#retry_timer_max   30  (integer or float)
#
expire_timer      600
retry_limit       10
retry_timer_init  2.5
retry_timer_max   180

```

Example 22-8 Shortening IKE Phase 1 Negotiation Times

In the following example, a system is connected to its IKE peers by a high-speed line with little traffic. The original settings are in comments in the file. The new settings shorten the negotiation time.

```
### ike/config file on partym
## Global Parameters
#
## Phase 1 transform defaults
#expire_timer 300
#retry_limit 5
#retry_timer_init 0.5 (integer or float)
#retry_timer_max 30 (integer or float)
#
expire_timer 120
retry_timer_init 0.20
```

Internet Key Exchange (Reference)

This chapter contains the following reference information about IKE:

- “IKE Daemon” on page 527
- “IKE Policy File” on page 528
- “IKE Administration Command” on page 528
- “IKE Preshared Keys Files” on page 529
- “IKE Public Key Databases and Commands” on page 530
- “IKE Status and Error Messages” on page 533

For instructions on implementing IKE, see [Chapter 22](#). For overview information, see [Chapter 21](#).

IKE Daemon

The `in.iked` daemon automates the management of cryptographic keys for IPsec on a Solaris system. The daemon negotiates with a remote system that is running the same protocol to provide authenticated keying materials for security associations (SAs) in a protected manner. The daemon must be running on all systems that plan to communicate securely.

The IKE daemon is automatically loaded at boot time if the configuration file for the IKE policy, `/etc/inet/ike/config`, exists. The daemon checks the syntax of the configuration file.

When the IKE daemon runs, the system authenticates itself to its peer IKE entity in the Phase 1 exchange. The peer is defined in the IKE policy file, as are the authentication methods. The daemon then establishes the keys for the Phase 2 exchange. At an interval specified in the policy file, the IKE keys are refreshed automatically. The `in.iked` daemon listens for incoming IKE requests from the network and for requests for outbound traffic through the `PF_KEY` socket. For more information, see the `pf_key(7P)` man page.

Two commands support the IKE daemon. The `ikeadm` command enables you to view and modify the IKE policy. The `ikecert` command enables you to view and manage the public key databases. This command manages the local databases, `ike.privatekeys` and `publickeys`. This command also manages public key operations and the storage of public keys on hardware.

IKE Policy File

The configuration file for the IKE policy, `/etc/inet/ike/config`, manages the keys for the interfaces that are being protected in the IPsec policy file, `/etc/inet/ipsecinit.conf`. The IKE policy file manages keys for IKE, and for the IPsec SAs. The IKE daemon itself requires keying material in the Phase 1 exchange.

Key management with IKE includes rules and global parameters. An IKE rule identifies the systems or networks that the keying material secures. The rule also specifies the authentication method. Global parameters include such items as the path to an attached hardware accelerator. For examples of IKE policy files, see [“Configuring IKE With Preshared Keys \(Task Map\)” on page 486](#). For examples and descriptions of IKE policy entries, see the `ike.config(4)` man page.

The IPsec SAs that IKE supports protect the IP datagrams according to policies that are set up in the configuration file for the IPsec policy, `/etc/inet/ipsecinit.conf`. The IKE policy file determines if perfect forward security (PFS) is used when creating the IPsec SAs.

The `ike/config` file can include the path to a library that is implemented according to the following standard: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). IKE uses this PKCS #11 library to access hardware for key acceleration and key storage.

The security considerations for the `ike/config` file are similar to the considerations for the `ipsecinit.conf` file. For details, see [“Security Considerations for ipsecinit.conf and ipsecconf” on page 471](#).

IKE Administration Command

You can use the `ikeadm` command to do the following:

- View aspects of the IKE daemon process.
- Change the parameters that are passed to the IKE daemon.

- Display statistics on SA creation during the Phase 1 exchange.
- Debug IKE processes.

For examples and a full description of this command's options, see the `ikeadm(1M)` man page. The privilege level of the running IKE daemon determines which aspects of the IKE daemon can be viewed and modified. You can choose from three levels of privilege.

0x0, or base level	You cannot view nor modify keying material. The base level is the default level at which the <code>in.iked</code> daemon runs.
0x1, or modkeys level	You can remove, change, and add preshared keys.
0x2, or keymat level	You can view the actual keying material with the <code>ikeadm</code> command.

The security considerations for the `ikeadm` command are similar to the considerations for the `ipseckey` command. For details, see [“Security Considerations for ipseckey” on page 473](#).

IKE Preshared Keys Files

When you create preshared keys manually, the keys are stored in files in the `/etc/inet/secret` directory. The `ike.preshared` file contains the preshared keys for Internet Security Association and Key Management Protocol (ISAKMP) SAs. The `ipseckey` file contains the preshared keys for IPsec SAs. The files are protected at 0600. The `secret` directory is protected at 0700.

- You create an `ike.preshared` file when you configure the `ike/config` file to require preshared keys. You enter keying material for ISAKMP SAs, that is, for IKE authentication, in the `ike.preshared` file. Because the preshared keys are used to authenticate the Phase 1 exchange, the file must be valid before the `in.iked` daemon starts.
- The `ipseckey` file contains keying material for IPsec SAs. For examples of manually managing the file, see [“How to Manually Create IPsec Security Associations” on page 461](#). The IKE daemon does not use this file. The keying material that IKE generates for IPsec SAs is stored in the kernel.

Note – Preshared keys cannot take advantage of hardware storage. Preshared keys are generated and are stored on the system.

IKE Public Key Databases and Commands

The `ikecert` command manipulates the local system's public key databases. You use this command when the `ike/config` file requires public key certificates. Because IKE uses these databases to authenticate the Phase 1 exchange, the databases must be populated before activating the `in.iked` daemon. Three subcommands handle each of the three databases: `certlocal`, `certdb`, and `certrldb`.

The `ikecert` command also handles key storage on the Sun Crypto Accelerator 4000 board. The `tokens` argument to the `ikecert` command lists the token IDs that are available on the board. The command finds the board through the PKCS #11 library that is specified in the `/etc/inet/ike/config` file. The PKCS #11 entry must be present. Otherwise, the `-T` option to the `ikecert` commands cannot work. The entry appears similar to the following:

```
pkcs11_path "/opt/SUNWconn/lib/libpkcs11.so"
```

For more information, see the `ikecert(1M)` man page.

`ikecert tokens` Command

The `tokens` argument lists the token IDs that are available on the Sun Crypto Accelerator 4000 board. Token IDs enable the `ikecert certlocal` and `ikecert certdb` commands to generate public key certificates and certificate requests on the board.

`ikecert certlocal` Command

The `certlocal` subcommand manages the private key database. Options to this subcommand enable you to add, view, and remove private keys. This subcommand also creates either a self-signed certificate or a certificate request. The `-ks` option creates a self-signed certificate. The `-kc` option creates a certificate request. Keys are stored on the system in the `/etc/inet/secret/ike.privatekeys` directory, or on attached hardware with the `-T` option.

When you create a private key, the options to the `ikecert certlocal` command must have related entries in the `ike/config` file. The correspondences between `ikecert` options and `ike/config` entries are shown in the following table.

TABLE 23-1 Correspondences Between `ikecert` Options and `ike/config` Entries

ikecert Option	ike/config Entry	Description
<code>-A subject-alternate-name</code>	<code>cert_trust</code> <code>subject-alternate-name</code>	A nickname that uniquely identifies the certificate. Possible values are an IP address, an email address, or a domain name.
<code>-D</code> <code>X.509-distinguished-name</code>	<code>X.509-distinguished-name</code>	The full name of the certificate authority that includes the country (C), organization name (ON), organizational unit (OU), and common name (CN).
<code>-t dsa-sha1</code>	<code>auth_method dss_sig</code>	An authentication method that is slightly slower than <i>RSA</i> .
<code>-t rsa-md5</code> and <code>-t rsa-sha1</code>	<code>auth_method rsa_sig</code>	An authentication method that is slightly faster than <i>DSA</i> . The RSA public key must be large enough to encrypt the biggest payload . Typically, an identity payload, such as the X.509 distinguished name, is the biggest payload.
<code>-t rsa-md5</code> and <code>-t rsa-sha1</code>	<code>auth_method rsa_encrypt</code>	RSA encryption hides identities in IKE from eavesdroppers, but requires that the IKE peers know each other's public keys.
<code>-T</code>	<code>pkcs11_path</code>	The PKCS #11 library handles key acceleration on the Sun Crypto Accelerator 1000 board and the Sun Crypto Accelerator 4000 board. The library also provides the tokens that handle key storage on the Sun Crypto Accelerator 4000 board.

If you issue a certificate request with the `ikecert certlocal -kc` command, you send the output of the command to a PKI organization or to a certificate authority (CA). If your company runs its own PKI, you send the output to your PKI administrator. The PKI organization, the CA, or your PKI administrator then creates certificates. The certificates that the PKI or CA returns to you are input to the `certdb` subcommand. The certificate revocation list (CRL) that the PKI returns to you is input for the `certrldb` subcommand.

ikecert certdb Command

The `certdb` subcommand manages the public key database. Options to this subcommand enable you to add, view, and remove certificates and public keys. The command accepts, as input, certificates that were generated by the `ikecert certlocal -ks` command on a remote system. For the procedure, see [“How to Configure IKE With Self-Signed Public Key Certificates”](#) on page 497. This command also accepts the certificate that you receive from a PKI or CA as input. For the procedure, see [“How to Configure IKE With Certificates Signed by a CA”](#) on page 501.

The certificates and public keys are stored on the system in the `/etc/inet/ike/publickeys` directory. The `-T` option stores the certificates, private keys, and public keys on attached hardware.

`ikecert certrldb` Command

The `certrldb` subcommand manages the certificate revocation list (CRL) database, `/etc/inet/ike/crls`. The CRL database maintains the revocation lists for public keys. Certificates that are no longer valid are on this list. When PKIs provide you with a CRL, you can install the CRL in the CRL database with the `ikecert certrldb` command. For the procedure, see [“How to Handle a Certificate Revocation List” on page 510](#).

`/etc/inet/ike/publickeys` Directory

The `/etc/inet/ike/publickeys` directory contains the public part of a public-private key pair and its certificate in files, or *slots*. The directory is protected at 0755. The `ikecert certdb` command populates the directory. The `-T` option stores the keys on the Sun Crypto Accelerator 4000 board rather than in the `publickeys` directory.

The slots contain, in encoded form, the X.509 distinguished name of a certificate that was generated on another system. If you are using self-signed certificates, you use the certificate that you receive from the administrator of the remote system as input to the command. If you are using certificates from a PKI, you install two pieces of keying material from the PKI into this database. You install a certificate that is based on material that you sent to the PKI. You also install a CA from the PKI.

`/etc/inet/secret/ike.privatekeys` Directory

The `/etc/inet/secret/ike.privatekeys` directory holds private key files that are part of a public-private key pair, which is keying material for ISAKMP SAs. The directory is protected at 0700. The `ikecert certlocal` command populates the `ike.privatekeys` directory. Private keys are not effective until their public key counterparts, self-signed certificates or CAs, are installed. The public key counterparts are stored in the `/etc/inet/ike/publickeys` directory or on a Sun Crypto Accelerator 4000 board.

`/etc/inet/ike/crls` Directory

The `/etc/inet/ike/crls` directory contains certificate revocation list (CRL) files. Each file corresponds to a public certificate file in the `/etc/inet/ike/publickeys` directory. PKI organizations provide the CRLs for their certificates. You can use the `ikecert certrldb` command to populate the database.

IKE Status and Error Messages

The `in.iked` daemon reports status and error codes about IKE negotiation. The following list describes the status codes.

8198	Delete notification
16384	Connected notification
24576	Responder lifetime notification
24577	Replay status notification
24578	Initial contact notification

The following list describes the error codes for IKE negotiation failures.

1	Invalid payload type
2	DOI not supported
3	Situation not supported
4	Invalid Cookie
5	Invalid IKE major version
6	Invalid IKE minor version
7	Invalid exchange type
8	Invalid flags
9	Invalid message ID
10	Invalid protocol ID
11	Invalid SPI
12	Invalid transform ID
13	Attributes not supported
14	No proposal chosen
15	Bad proposal syntax
16	Payload malformed
17	Invalid key information
18	Invalid ID information
19	Invalid certificate encoding
20	Invalid certificate

21	Certificate type unsupported
22	Invalid certificate authority
23	Invalid hash information
24	Authentication failed
25	Invalid signature
28	Certificate unavailable
29	Unsupported exchange type
30	Payload lengths do not match
8194	No SA established
8195	State not matched
8196	Exchange data missing
8197	Timeout
8199	Aborted notification
8200	UDP host unreachable
8201	UDP port unreachable

Solaris IP Filter (Overview)

This chapter provides an overview of Solaris IP Filter. For Solaris IP Filter tasks, see [Chapter 25](#).

This chapter contains the following information:

- “Introduction to Solaris IP Filter” on page 535
- “Guidelines for Using Solaris IP Filter” on page 536
- “Using Solaris IP Filter Configuration Files” on page 536
- “Working With Solaris IP Filter Rule Sets” on page 537
- “Activating Solaris IP Filter Using the `pfil` STREAMS Module” on page 542
- “Solaris IP Filter Man Pages” on page 543

Introduction to Solaris IP Filter

Solaris IP Filter replaces the SunScreen™ firewall as the firewall software for the Solaris Operating System (Solaris OS). Like the SunScreen firewall, Solaris IP Filter provides stateful packet filtering and network address translation (NAT). Solaris IP Filter also includes stateless packet filtering and the ability to create and manage address pools.

Packet filtering provides basic protection against network-based attacks. Solaris IP Filter can filter by IP address, port, protocol, network interface, and traffic direction. Solaris IP Filter can also filter by an individual source IP address, a destination IP address, by a range of IP addresses, or by address pools.

Solaris IP Filter is derived from open source IP Filter software. To view license terms, attribution, and copyright statements for open source IP Filter, the default path is `/usr/lib/ipf/IPFILTER.LICENCE`. If the Solaris OS has been installed anywhere other than the default, modify the given path to access the file at the installed location.

Information Sources for Open Source IP Filter

The home page for the open source IP Filter software by Darren Reed is found at <http://coombs.anu.edu.au/~avalon/ip-filter.html>. This site includes information for open source IP Filter, including a link to a tutorial entitled “IP Filter Based Firewalls HOWTO” (Brendan Conoboy and Erik Fichtner, 2002). This tutorial provides step-by-step instructions for building firewalls in a BSD UNIX environment.

Guidelines for Using Solaris IP Filter

- Solaris IP Filter is managed by the SMF services `svc:/network/pfil` and `svc:/network/ipfilter`. For a complete overview of SMF, see Chapter 9, “Managing Services (Overview),” in *System Administration Guide: Basic Administration*. For information on the step-by-step procedures that are associated with SMF, see Chapter 14, “Managing Services (Tasks),” in *System Administration Guide: Basic Administration*.
 - Solaris IP Filter requires direct editing of configuration files.
 - Solaris IP Filter is installed as part of the Solaris OS. By default, Solaris IP Filter is not activated after a fresh install. To configure filtering, you must edit configuration files and manually activate Solaris IP Filter. You can activate filtering by either rebooting the system or by plumbing the interfaces using the `ifconfig` command. For more information, see the `ifconfig(1M)` man page. For the tasks associated with enabling Solaris IP Filter, see “Configuring Solaris IP Filter” on page 545.
 - To administer Solaris IP Filter, you must be able to assume a role that includes the IP Filter Management rights profile, or become superuser. You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.
 - IP Network Multipathing (IPMP) supports stateless filtering only.
 - Sun Cluster configurations do not support filtering with Solaris IP Filter.
-

Using Solaris IP Filter Configuration Files

Solaris IP Filter can be used to provide firewall services or network address translation (NAT). Solaris IP Filter can be implemented using loadable configuration files. Solaris IP Filter includes a directory called `/etc/ipf`. You can create and store configuration files called `ipf.conf`, `ipnat.conf` and `ippool.conf` in the `/etc/ipf` directory.

These files are loaded automatically during the boot process when they reside in the `/etc/ipf` directory. You can also store the configuration files in another location and load the files manually. For example configuration files, see [“Creating and Editing Solaris IP Filter Configuration Files”](#) on page 572.

Working With Solaris IP Filter Rule Sets

To manage your firewall, you use Solaris IP Filter to specify rule sets that you use to filter your network traffic. You can create the following types of rule sets:

- Packet filtering rule sets
- Network Address Translation (NAT) rule sets

Additionally, you can create address pools to reference groups of IP addresses. You can then use these pools later in a rule set. The address pools help to speed up rule processing. Address pools also make managing large groups of addresses easier.

Using Solaris IP Filter’s Packet Filtering Feature

You set up packet filtering by using packet filtering rule sets. Use the `ipf` command to work with packet filtering rule sets. For more information on the `ipf` command, see the `ipf(1M)` command.

You can create packet filtering rules either at the command line, using the `ipf` command, or in a packet filtering configuration file. If you want the packet filtering rules to be loaded at boot time, create a configuration file called `/etc/ipf/ipf.conf` in which to put packet filtering rules. If you do not want the packet filtering rules loaded at boot time, put the `ipf.conf` file in a location of your choice, and manually activate packet filtering by using the `ipf` command.

You can maintain two sets of packet filtering rule sets with Solaris IP Filter, the active rule set and the inactive rule set. In most cases, you work with the active rule set. However, the `ipf -I` command enables you to apply the command action to the inactive rule list. The inactive rule list is not used by Solaris IP Filter unless you select it. The inactive rule list provides you with a place to store rules without affecting active packet filtering.

Solaris IP Filter processes the rules in the rules list from the beginning of the configured rules list to the end of the rules list before passing or blocking a packet. Solaris IP Filter maintains a flag that determines whether it will or will not pass a packet. It goes through the entire rule set and determines whether to pass or block the packet based on the last matching rule.

There are two exceptions to this process. The first exception is if the packet matches a rule containing the `quick` keyword. If a rule includes the `quick` keyword, the action for that rule is taken, and no subsequent rules are checked. The second exception is if the packet matches a rule containing the `group` keyword. If a packet matches a group, only rules tagged with the `group` are checked.

Configuring Packet Filtering Rules

Use the following syntax to create packet filtering rules:

action [*in|out*] *option keyword, keyword...*

1. Each rule begins with an action. Solaris IP Filter applies the action to the packet if the packet matches the rule. The following list includes the commonly used actions applied to a packet.

<code>block</code>	Prevents the packet from passing through the filter.
<code>pass</code>	Allows the packet through the filter.
<code>log</code>	Logs the packet but does not determine if the packet is blocked or passed. Use the <code>ipmon</code> command to view the log.
<code>count</code>	Includes the packet in the filter statistics. Use the <code>ipfstat</code> command to view the statistics.
<code>skip number</code>	Makes the filter skip over <i>number</i> filtering rules.
<code>auth</code>	Requests that packet authentication be performed by a user program that validates packet information. The program determines whether the packet is passed or blocked.
<code>preauth</code>	Requests that the filter look at a pre-authenticated list to determine what to do with the packet.

2. Following the action, the next word must be either `in` or `out`. Your choice determines whether the packet filtering rule is applied to an incoming packet or to an outgoing packet.
3. Next, you can choose from a list of options. If you use more than one option, they must be in the order shown here.

<code>log</code>	Logs the packet if the rule is the last matching rule. Use the <code>ipmon</code> command to view the log.
<code>quick</code>	Executes the rule containing the <code>quick</code> option if there is a packet match. All further rule checking stops.
<code>on interface-name</code>	Applies the rule only if the packet is moving in or out of the specified interface.
<code>dup-to interface-name</code>	Copies the packet and sends the duplicate out on <i>interface-name</i> to an optionally specified IP address.

`to interface-name` Moves the packet to an outbound queue on `interface-name`.

4. After specifying the options, you can choose from a variety of keywords that determine whether the packet matches the rule. The following keywords must be used in the order shown here.

`tos` Filters the packet based on the type-of-service value expressed as either a hexadecimal or a decimal integer.

`ttl` Matches the packet based on its time-to-live value. The time-to-live value stored in a packet indicates the length of time a packet can be on the network before being discarded.

`proto` Matches a specific protocol. You can use any of the protocol names specified in the `/etc/protocols` file, or use a decimal number to represent the protocol. The keyword `tcp/udp` can be used to match either a TCP or a UDP packet.

`from/to/all/any` Matches any or all of the following: the source IP address, the destination IP address, and the port number. The `all` keyword is used to accept packets from all sources and to all destinations.

`with` Matches specified attributes associated with the packet. Insert either the word `not` or the word `no` in front of the keyword in order to match the packet only if the option is not present.

`flags` Used for TCP to filter based on TCP flags that are set. For more information on the TCP flags, see the `ipf(4)` man page.

`icmp-type` Filters according to ICMP type. This keyword is used only when the `proto` option is set to `icmp` and is not used if the `flags` option is used.

`keep keep-options` Determines the information that is kept for a packet. The `keep-options` available include the `state` option and the `frags` option. The `state` option keeps information about the session and can be kept on TCP, UDP, and ICMP packets. The `frags` option keeps information on packet fragments and applies the information to later fragments. The `keep-options` allow matching packets to pass without going through the access control list.

`head number` Creates a new group for filtering rules, which is denoted by the number `number`.

`group number` Adds the rule to group number `number` instead of the default group. All filtering rules are placed in group 0 if no other group is specified.

The following example illustrates how to put together the packet filtering rule syntax to create a rule. To block incoming traffic from the IP address 192.168.0.0/16, you would include the following rule in the rule list:

```
block in quick from 192.168.0.0/16 to any
```

For the complete grammar and syntax used to write packet filtering rules, see the `ipf(4)` man page. For tasks associated with packet filtering, see [“Managing Packet Filtering Rule Sets for Solaris IP Filter” on page 555](#). For an explanation of the IP address scheme (192.168.0.0/16) shown in the example, see [Chapter 2](#).

Using Solaris IP Filter’s NAT Feature

NAT sets up mapping rules that translate source and destination IP addresses into other Internet or intranet addresses. These rules modify the source and destination addresses of incoming or outgoing IP packets and send the packets on. You can also use NAT to redirect traffic from one port to another port. NAT maintains the integrity of the packet during any modification or redirection done on the packet.

Use the `ipnat` command to work with NAT rule lists. For more information on the `ipnat` command, see the `ipnat(1M)` command.

You can create NAT rules either at the command line, using the `ipnat` command, or in a NAT configuration file. NAT configuration rules reside in the `ipnat.conf` file. If you want the NAT rules to be loaded at boot time, create a file called `/etc/ipf/ipnat.conf` in which to put NAT rules. If you do not want the NAT rules loaded at boot time, put the `ipnat.conf` file in a location of your choice, and manually activate packet filtering with the `ipnat` command.

Configuring NAT Rules

Use the following syntax to create NAT rules:

command interface-name parameters

1. Each rule begins with one of the following commands:

<code>map</code>	Maps one IP address or network to another IP address or network in an unregulated round-robin process.
<code>rdr</code>	Redirects packets from one IP address and port pair to another IP address and port pair.
<code>bimap</code>	Establishes a bidirectional NAT between an external IP address and an internal IP address.

`map-block` Establishes static IP address-based translation. This command is based on an algorithm that forces addresses to be translated into a destination range.

2. Following the command, the next word is the interface name, such as `hme0`.
3. Next, you can choose from a variety of parameters, which determine the NAT configuration. Some of the parameters include:

`ipmask` Designates the network mask.

`dstipmask` Designates the address that `ipmask` is translated to.

`mapport` Designates `tcp`, `udp`, or `tcp/udp` protocols, along with a range of port numbers.

The following example illustrates how to put together the NAT rule syntax together to create a NAT rule. To rewrite a packet that goes out on the `de0` device with a source address of `192.168.1.0/24` and to externally show its source address as `10.1.0.0/16`, you would include the following rule in the NAT rule set:

```
map de0 192.168.1.0/24 -> 10.1.0.0/16
```

For the complete grammar and syntax used to write NAT rules, see the `ipnat(4)` man page.

Using Solaris IP Filter's Address Pools Feature

Address pools establish a single reference that is used to name a group of address/netmask pairs. Address pools provide processes to reduce the time needed to match IP addresses with rules. Address pools also make managing large groups of addresses easier.

Address pool configuration rules reside in the `ippool.conf` file. If you want the address pool rules to be loaded at boot time, create a file called `/etc/ipf/ippool.conf` in which to put address pool rules. If you do not want the address pool rules loaded at boot time, put the `ippool.conf` file in a location of your choice, and manually activate packet filtering with the `ippool` command.

Configuring Address Pools

Use the following syntax to create an address pool:

```
table role = role-name type = storage-format number = reference-number
```

`table` Defines the reference for the multiple addresses.

`role` Specifies the role of the pool in Solaris IP Filter. At this time, the only role you can reference is `ipf`.

`type` Specifies the storage format for the pool.
`number` Specifies the reference number that is used by the filtering rule.

For example, to reference the group of addresses 10.1.1.1 and 10.1.1.2, and the network 192.16.1.0 as pool number 13, you would include the following rule in the address pool configuration file:

```
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24 };
```

Then, to reference pool number 13 in a filtering rule, you would construct the rule similar to the following example:

```
pass in from pool/13 to any
```

Note that you must load the pool file before loading the rules file that contains a reference to the pool. If you do not, the pool is undefined, as shown in the following output:

```
# ipfstat -io
empty list for ipfilter(out)
block in from pool/13(!) to any
```

Even if you add the pool later, the addition of the pool does not update the kernel rule set. You also need to reload the rules file that references the pool.

For the complete grammar and syntax used to write packet filtering rules, see the `ippool(4)` man page.

Activating Solaris IP Filter Using the `pfil` STREAMS Module

The `pfil` STREAMS module is required to enable Solaris IP Filter. However, Solaris IP Filter does not provide an automatic mechanism to push the module on to every interface. Instead, the `pfil` STREAMS module is managed by the SMF service `svc:/network/pfil`. To activate filtering on a network interface, you configure the `pfil.ap` file and activate the `svc:/network/pfil` service to supply the `pfil` STREAMS module to the network interface. For the STREAMS module to take effect, the system must be rebooted or each network interface on which you want filtering must be unplumbed and then re-plumbed. For tasks associated with activating Solaris IP Filter, see [“Configuring Solaris IP Filter” on page 545](#).

Solaris IP Filter Man Pages

The following table includes the man page documentation relevant to Solaris IP Filter.

Man Page	Description
<code>ipf(1M)</code>	Use the <code>ipf</code> command to complete the following tasks: <ul style="list-style-type: none">■ Work with packet filtering rule sets.■ Disable and enable filtering.■ Reset statistics and resynchronize the in-kernel interface list with the current interface status list.
<code>ipf(4)</code>	Contains the grammar and syntax for creating Solaris IP Filter packet filtering rules.
<code>ipfilter(5)</code>	Provides open source IP Filter licensing information.
<code>ipfs(1M)</code>	Use the <code>ipfs</code> command to save and restore NAT information and state table information across reboots.
<code>ipfstat(1M)</code>	Use the <code>ipfstat</code> command to retrieve and display statistics on packet processing.
<code>ipmon(1M)</code>	Use the <code>ipmon</code> command to open the log device and view logged packets for both packet filtering and NAT.
<code>ipnat(1M)</code>	Use the <code>ipnat</code> command to complete the following tasks: <ul style="list-style-type: none">■ Work with NAT rules.■ Retrieve and display NAT statistics.
<code>ipnat(4)</code>	Contains the grammar and syntax for creating NAT rules.
<code>ippool(1M)</code>	Use the <code>ippool</code> command to create and manage address pools.
<code>ippool(4)</code>	Contains the grammar and syntax for creating Solaris IP Filter address pools.
<code>ndd(1M)</code>	Displays current filtering parameters of the <code>pfil</code> STREAMS module and the current values of the tunable parameters.

Solaris IP Filter (Tasks)

This chapter provides step-by-step instructions for Solaris IP Filter tasks. For overview information on Solaris IP Filter, see [Chapter 24](#).

This chapter contains the following information:

- “Configuring Solaris IP Filter” on page 545
- “Deactivating and Disabling Solaris IP Filter” on page 550
- “Working With Solaris IP Filter Rule Sets” on page 554
- “Displaying Statistics and Information for Solaris IP Filter” on page 565
- “Working With Log Files for Solaris IP Filter” on page 569
- “Creating and Editing Solaris IP Filter Configuration Files” on page 572

Configuring Solaris IP Filter

The following task map identifies the procedures associated with configuring Solaris IP Filter.

TABLE 25–1 Configuring Solaris IP Filter (Task Map)

Task	Description	For Instructions
Initially enable Solaris IP Filter.	Solaris IP Filter is not enabled by default. You must either enable it manually or configure the <code>/etc/ipf/ipf.conf</code> file and reboot the system.	“How to Enable Solaris IP Filter” on page 546

TABLE 25-1 Configuring Solaris IP Filter (Task Map) *(Continued)*

Task	Description	For Instructions
Re-enable Solaris IP Filter.	If Solaris IP Filter is deactivated or disabled, you can re-enable Solaris IP Filter either by rebooting the system or by using the <code>ipf</code> command.	“How to Re-Enable Solaris IP Filter” on page 548
Activate a specific network interface card (NIC) for packet filtering.	You can activate a NIC and allow Solaris IP Filter to filter packets on that NIC.	“How to Activate a NIC for Packet Filtering” on page 549

▼ How to Enable Solaris IP Filter

Solaris IP Filter is installed with the Solaris Operating System (Solaris OS). However, packet filtering is not enabled by default. Use the following procedure to activate Solaris IP Filter.

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see *“Configuring RBAC (Task Map)”* in *System Administration Guide: Security Services*.

2. **Start the file editor of your choice, and edit the `/etc/ipf/pfil.ap` file.**

This file contains the names of network interface cards (NICs) on the host. By default, the names are commented out. Uncomment the device names that carry the network traffic you want to filter.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor  lastminor  modules

#le     -1     0         pfil
#qe     -1     0         pfil
hme     -1     0         pfil (Device has been uncommented for filtering)
#qfe    -1     0         pfil
#eri    -1     0         pfil
#ce     -1     0         pfil
#bge    -1     0         pfil
#be     -1     0         pfil
#vge    -1     0         pfil
```

```
#ge      -1      0      pfil
#nf      -1      0      pfil
#fa      -1      0      pfil
#ci      -1      0      pfil
#el      -1      0      pfil
#ipdptp -1      0      pfil
#lane    -1      0      pfil
#dmfe    -1      0      pfil
```

3. Activate your changes to the `/etc/ipf/pfil.ap` file by restarting the `network/pfil` service instance.

```
# svcadm restart network/pfil
```

4. Create a packet filtering rule set.

The packet filtering configuration file contains packet filtering rules that are used by Solaris IP Filter. If you want the packet filtering rules to be loaded at boot time, edit the `/etc/ipf/ipf.conf` file. If you do not want the packet filtering rules loaded at boot time, put the rules in a file of your choice, and manually activate packet filtering. For information on packet filtering, see [“Using Solaris IP Filter’s Packet Filtering Feature” on page 537](#). For information on working with configuration files, see [“Creating and Editing Solaris IP Filter Configuration Files” on page 572](#).

5. (Optional) Create a network address translation (NAT) configuration file.

Create an `ipnat.conf` file if you want to use network address translation. If you want the NAT rules to be loaded at boot time, create a file called `/etc/ipf/ipnat.conf` in which to put NAT rules. If you do not want the NAT rules loaded at boot time, put the `ipnat.conf` file in a location of your choice, and manually activate the NAT rules.

For more information on NAT, see [“Using Solaris IP Filter’s NAT Feature” on page 540](#).

6. (Optional) Create an address pool configuration file.

Create an `ipool.conf` file if you want to refer to a group of addresses as a single address pool. If you want the address pool configuration file to be loaded at boot time, create a file called `/etc/ipf/ippool.conf` in which to put the address pool. If you do not want the address pool configuration file to be loaded at boot time, put the `ippool.conf` file in a location of your choice, and manually activate the rules.

For more information on address pools, see [“Using Solaris IP Filter’s Address Pools Feature” on page 541](#).

7. Enable Solaris IP Filter.

```
# svcadm enable network/ipfilter
```

8. Activate Solaris IP Filter using one of the following methods:

- Reboot the machine.

```
# reboot
```

Note – Rebooting is required if you cannot safely use the `ifconfig unplumb` and `ifconfig plumb` commands on the NICs.

- Enable the NICs using the `ifconfig` command with the `unplumb` and `plumb` options.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f840::1/96 up
```

For more information on the `ifconfig` command, see the `ifconfig(1M)` man page.

Note – The `inet6` version of each interface must also be plumbed in order to block IPv6 traffic. Although the present version of Solaris IP Filter does not apply filtering rules to IPv6 traffic, it will block all IPv6 packets to prevent IPv6-based attacks.

▼ How to Re-Enable Solaris IP Filter

You can re-enable packet filtering after it has been temporarily disabled.

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Enable Solaris IP Filter and activate filtering using one of the following methods:**

- Reboot the machine.

```
# reboot
```

Note – If you reboot your system, the packet filtering rules in the `/etc/ipf/ipf.conf` file and the `/etc/ipf/ipnat.conf` file are activated.

- Perform the following series of commands to enable Solaris IP Filter and activate filtering:

- a. Enable Solaris IP Filter.

```
# ipf -E
```

- b. Activate packet filtering.

```
# ipf -f filename
```

- c. (Optional) Activate NAT.

```
# ipnat -f filename
```

▼ How to Activate a NIC for Packet Filtering

Solaris IP Filter is enabled at boot time when the `/etc/ipf/ipf.conf` file exists. If you need to enable filtering on a NIC after Solaris IP Filter is enabled, use the following procedure.

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Start the file editor of your choice, and edit the `/etc/ipf/pfil.ap` file.**

This file contains the names of NICs on the host. By default, the names are commented out. Uncomment the device names that carry the network traffic you want to filter.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor  lastminor  modules

#le      -1      0          pfil
#qe      -1      0          pfil
hme      -1      0          pfil (Device has been uncommented for filtering)
#qfe     -1      0          pfil
#eri     -1      0          pfil
#ce      -1      0          pfil
#bge     -1      0          pfil
#be      -1      0          pfil
#vge     -1      0          pfil
#ge      -1      0          pfil
#nf      -1      0          pfil
#fa      -1      0          pfil
#ci      -1      0          pfil
```

```
#el      -1      0      pfil
#ipdptp -1      0      pfil
#lane   -1      0      pfil
#dmfe   -1      0      pfil
```

3. Activate your changes to the `/etc/ipf/pfil.ap` file by restarting the `network/pfil` service instance.

```
# svcadm restart network/pfil
```

4. Enable the NIC using one of the following methods:

- Reboot the machine.

```
# reboot
```

Note – Rebooting is required if you cannot safely use the `ifconfig unplumb` and `ifconfig plumb` commands on the NICs.

- Enable the NICs that you want to filter using the `ifconfig` command with the `unplumb` and `plumb` options.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f840::1/96 up
```

For more information on the `ifconfig` command, see the `ifconfig(1M)` man page.

Note – The `inet6` version of each interface must also be plumbed in order to block IPv6 traffic. Although the present version of Solaris IP Filter does not apply filtering rules to IPv6 traffic, it will block all IPv6 packets to prevent IPv6-based attacks.

Deactivating and Disabling Solaris IP Filter

You might want to deactivate or disable packet filtering and NAT under the following circumstances:

- For testing purposes
- To troubleshoot system problems when you think the problems are caused by Solaris IP Filter

The following task map identifies the procedures associated with deactivating or disabling Solaris IP Filter features.

TABLE 25-2 Deactivating and Disabling Solaris IP Filter (Task Map)

Task	Description	For Instructions
Deactivate packet filtering.	Deactivate packet filtering using the <code>ipf</code> command.	“How to Deactivate Packet Filtering” on page 551
Deactivate NAT.	Deactivate NAT using the <code>ipnat</code> command.	“How to Deactivate NAT” on page 552
Deactivate Solaris IP Filter on a NIC.	Remove a NIC and allow all packets to pass through the NIC.	“How to Deactivate Solaris IP Filter on a NIC” on page 552
Disable packet filtering and NAT.	Disable packet filtering and NAT using the <code>ipf</code> command.	“How to Disable Packet Filtering” on page 554

▼ How to Deactivate Packet Filtering

The following procedure deactivates Solaris IP Filter packet filtering by flushing the packet filtering rules from the active filtering rule set. The procedure does not disable Solaris IP Filter. You can reactivate Solaris IP Filter by adding rules to the rule set.

- Steps**
- 1. Assume a role that includes the IP Filter Management rights profile, or become superuser.**
You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see *“Configuring RBAC (Task Map)”* in *System Administration Guide: Security Services*.
 - 2. Use one of the following methods to deactivate Solaris IP Filter rules:**
 - Remove the active rule set from the kernel.

```
# ipf -Fa
```

This command deactivates all packet filtering rules.
 - Remove incoming packet filtering rules.

```
# ipf -Fi
```

This command deactivates packet filtering rules for incoming packets.
 - Remove outgoing packet filtering rules.

```
# ipf -Fo
```

This command deactivates packet filtering rules for outgoing packets.

▼ How to Deactivate NAT

The following procedure deactivates Solaris IP Filter NAT rules by flushing the NAT rules from the active NAT rules set. The procedure does not disable Solaris IP Filter. You can reactivate Solaris IP Filter by adding rules to the rule set.

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Remove NAT from the kernel.**

```
# ipnat -FC
```

The `-C` option removes all entries in the current NAT rule listing. The `-F` option removes all active entries in the current NAT translation table, which shows the currently active NAT mappings.

▼ How to Deactivate Solaris IP Filter on a NIC

If you need to stop filtering packets on a NIC, use the following procedure.

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Start the file editor of your choice, and edit the `/etc/ipf/pfil.ap` file.**

This file contains the names of NICs on the host. The NICs that have been used to filter network traffic are uncommented. Comment out the device names that you no longer want to use to filter network traffic.

```
# vi /etc/ipf/pfil.ap
# IP Filter pfil autopush setup
#
# See autopush(1M) manpage for more information.
#
# Format of the entries in this file is:
#
#major  minor  lastminor  modules

#le     -1     0         pfil
#qe     -1     0         pfil
#hme    -1     0         pfil (Device has been commented out to no longer filter network traffic)
#qfe    -1     0         pfil
```



```
#eri -1 0 pfil
#ce -1 0 pfil
#bge -1 0 pfil
#be -1 0 pfil
#vge -1 0 pfil
#ge -1 0 pfil
#nf -1 0 pfil
#fa -1 0 pfil
#ci -1 0 pfil
#el -1 0 pfil
#ipdptp -1 0 pfil
#lane -1 0 pfil
#dmfe -1 0 pfil
```

3. Activate your changes to the `/etc/ipf/pfil.ap` file by restarting the `network/pfil` service instance.

```
# svcadm restart network/pfil
```

4. Deactivate the NIC using one of the following methods:

- Reboot the machine.

```
# reboot
```

Note – Rebooting is required if you cannot safely use the `ifconfig unplumb` and `ifconfig plumb` commands on the NICs.

- Deactivate the NICs using the `ifconfig` command with the `unplumb` and `plumb` options.

```
# ifconfig hme0 unplumb
# ifconfig hme0 plumb 192.168.1.20 netmask 255.255.255.0 up
# ifconfig hme0 inet6 unplumb
# ifconfig hme0 inet6 plumb fec3:f840::1/96 up
```

For more information on the `ifconfig` command, see the `ifconfig(1M)` man page.

Note – The `inet6` version of each interface must also be plumbed in order to block IPv6 traffic. Although the present version of Solaris IP Filter does not apply filtering rules to IPv6 traffic, it will block all IPv6 packets to prevent IPv6-based attacks.

▼ How to Disable Packet Filtering

When you run this procedure, both packet filtering and NAT are removed from the kernel. If you use this procedure, you must re-enable Solaris IP Filter in order to reactivate packet filtering and NAT. For more information, see [“How to Re-Enable Solaris IP Filter”](#) on page 548.

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see [“Configuring RBAC \(Task Map\)”](#) in *System Administration Guide: Security Services*.

2. **Disable packet filtering and allow all packets to pass into the network.**

```
# ipf -D
```

Working With Solaris IP Filter Rule Sets

The following task map identifies the procedures associated with Solaris IP Filter rule sets.

TABLE 25-3 Working With Solaris IP Filter Rule Sets (Task Map)

Task	Description	For Instructions
Manage, view and modify Solaris IP Filter packet filtering rule sets.		“Managing Packet Filtering Rule Sets for Solaris IP Filter” on page 555
	View an active packet filtering rule set.	“How to View the Active Packet Filtering Rule Set” on page 556
	View an inactive packet filtering rule set.	“How to View the Inactive Packet Filtering Rule Set” on page 556
	Activate a different active rule set.	“How to Activate a Different Packet Filtering Rule Set” on page 556
	Remove a rule set.	“How to Remove a Packet Filtering Rule Set” on page 557

TABLE 25-3 Working With Solaris IP Filter Rule Sets (Task Map) *(Continued)*

Task	Description	For Instructions
	Add rules to the rule sets.	<p>“How to Append Rules to the Active Packet Filtering Rule Set” on page 558</p> <p>“How to Append Rules to the Inactive Packet Filtering Rule Set” on page 559</p>
	Move between active and inactive rule sets.	“How to Switch Between Active and Inactive Packet Filtering Rule Sets” on page 559
	Delete an inactive rule set from the kernel.	“How to Remove an Inactive Packet Filtering Rule Set From the Kernel” on page 560
Manage, view and modify Solaris IP Filter NAT rules.		“Managing NAT Rules for Solaris IP Filter” on page 561
	View active NAT rules.	“How to View Active NAT Rules” on page 561
	Remove NAT rules.	“How to Remove NAT Rules” on page 562
Manage, view and modify Solaris IP Filter address pools.	Add additional rules to NAT rules.	“How to Append Rules to the NAT Rules” on page 562
	View active address pools.	“How to View Active Address Pools” on page 563
	Remove an address pool.	“How to Remove an Address Pool” on page 564
	Add additional rules to an address pool.	“How to Append Rules to an Address Pool” on page 564

Managing Packet Filtering Rule Sets for Solaris IP Filter

When Solaris IP Filter is enabled, both active and inactive packet filtering rule sets can reside in the kernel. The active rule set determines what filtering is being done on incoming packets and outgoing packets. The inactive rule set also stores rules. These rules are not used unless you make the inactive rule set the active rule set. You can manage, view, and modify both active and inactive packet filtering rule sets.

▼ How to View the Active Packet Filtering Rule Set

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**
You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **View the active packet filtering rule set that is loaded in the kernel.**

```
# ipfstat -io
```

Example 25–1 Viewing the Active Packet Filtering Rule Set

The following example shows output from the active packet filtering rule set that is loaded in the kernel.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe1 from 192.168.1.0/24 to any
pass in all
block in on dmfe1 from 192.168.1.10/32 to any
```

▼ How to View the Inactive Packet Filtering Rule Set

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**
You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **View the inactive packet filtering rule set.**

```
# ipfstat -I -io
```

Example 25–2 Viewing the Inactive Packet Filtering Rule Set

The following example shows output from the inactive packet filtering rule set.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
```

▼ How to Activate a Different Packet Filtering Rule Set

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. Create a new rule set in a file of your choice, or edit the rule set in the `/etc/ipf/ipf.conf` file.
3. Remove the current rule set and load the new rule set.

```
# ipf -Fa -f filename
```

The active rule set is removed from the kernel. The rules in the *filename* file become the active rule set.

Example 25–3 Activating a Different Packet Filtering Rule Set

The following example shows how to replace one packet filtering rule set with another packet filtering rule set.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe all
# ipf -Fa -f /etc/ipf/ipf.conf
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
```

▼ How to Remove a Packet Filtering Rule Set

- Steps**
1. Assume a role that includes the IP Filter Management rights profile, or become superuser.

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. Remove the rule set.

```
# ipf -F [a|i|o]
```

- a Removes all filtering rules from the rule set.
- i Removes the filtering rules for incoming packets.
- o Removes the filtering rules for outgoing packets.

Example 25–4 Removing a Packet Filtering Rule Set

The following example shows how to remove all filtering rules from the active filtering rule set.

```
# ipfstat -io
block out log on dmf0 all
```

```
block in log quick from 10.0.0.0/8 to any
# ipf -Fa
# ipfstat -io
empty list for ipfilter(out)
empty list for ipfilter(in)
```

▼ How to Append Rules to the Active Packet Filtering Rule Set

- Steps** 1. Assume a role that includes the IP Filter Management rights profile, or become superuser.

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. Use one of the following methods to append rules to the active rule set:

- Append rules to the rule set at the command line using the `ipf -f -` command.

```
# echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
```

- Perform the following commands:

- a. Create a rule set in a file of your choice.
- b. Add the rules you have created to the active rule set.

```
# ipf -f filename
```

The rules in *filename* are added to the end of the active rule set. Because Solaris IP Filter uses a “last matching rule” algorithm, the added rules determine filtering priorities, unless you use the `quick` keyword. If the packet matches a rule containing the `quick` keyword, the action for that rule is taken, and no subsequent rules are checked.

Example 25–5 Appending Rules to the Active Packet Filtering Rule Set

The following example shows how to add a rule to the active packet filtering rule set from the command line.

```
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
# echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

▼ How to Append Rules to the Inactive Packet Filtering Rule Set

- Steps** 1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Create a rule set in a file of your choice.**
3. **Add the rules you have created to the inactive rule set.**

```
# ipf -I -f filename
```

The rules in *filename* are added to the end of the inactive rule set. Because Solaris IP Filter uses a “last matching rule” algorithm, the added rules determine filtering priorities, unless you use the `quick` keyword. If the packet matches a rule containing the `quick` keyword, the action for that rule is taken, and no subsequent rules are checked.

Example 25–6 Appending Rules to the Inactive Rule Set

The following example shows how to add a rule to the inactive rule set from a file.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
# ipf -I -f /etc/ipf/ipf.conf
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

▼ How to Switch Between Active and Inactive Packet Filtering Rule Sets

- Steps** 1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Switch the active and inactive rule sets.**

```
# ipf -s
```

This command enables you to switch between the active and inactive rule sets in the kernel. Note that if the inactive rule set is empty, there is no packet filtering.

Example 25–7 Switching Between the Active and Inactive Packet Filtering Rule Sets

The following example shows how using the `ipf -s` command results in the inactive rule set becoming the active rule set and the active rule set becoming the inactive rule set.

- Before running the `ipf -s` command, the output from the `ipfstat -I -io` command shows the rules in the inactive rule set. The output from the `ipfstat -io` command shows the rules in the active rule set.

```
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

- After running the `ipf -s` command, the output from the `ipfstat -I -io` and the `ipfstat -io` command show that the content of the two rules sets have switched.

```
# ipf -s
Set 1 now inactive
# ipfstat -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

▼ How to Remove an Inactive Packet Filtering Rule Set From the Kernel

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. Specify the inactive rule set in the “flush all” command.

```
# ipf -I -Fa
```

This command flushes the inactive rule set from the kernel.

Note – If you subsequently run `ipf -s`, the empty inactive rule set will become the active rule set. An empty active rule set means that *no* filtering will be done.

Example 25–8 Removing an Inactive Packet Filtering Rule Set From the Kernel

The following example shows how to flush the inactive packet filtering rule set so that all rules have been removed.

```
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
# ipf -I -Fa
# ipfstat -I -io
empty list for inactive ipfilter(out)
empty list for inactive ipfilter(in)
```

Managing NAT Rules for Solaris IP Filter

Use the following procedures to manage, view, and modify NAT rules.

▼ How to View Active NAT Rules

- Steps**
1. Assume a role that includes the IP Filter Management rights profile, or become superuser.

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. View the active NAT rules.

```
# ipnat -l
```

Example 25–9 Viewing Active NAT Rules

The following example shows the output from the active NAT rules set.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

▼ How to Remove NAT Rules

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Remove the current NAT rules.**

```
# ipnat -C
```

Example 25-10 Removing NAT Rules

The following example shows how to remove the entries in the current NAT rules.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
# ipnat -C
1 entries flushed from NAT list
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
```

▼ How to Append Rules to the NAT Rules

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Use one of the following methods to append rules to the active rule set:**

- Append rules to the NAT rule set at the command line using the `ipnat -f -` command.

```
# echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
```

- Perform the following commands:
 - a. Create additional NAT rules in a file of your choice.
 - b. Add the rules you have created to the active NAT rules.

```
# ipnat -f filename
```

The rules in *filename* are added to the end of the NAT rules.

Example 25-11 Appending Rules to the NAT Rule Set

The following example shows how to add a rule to the NAT rule set from the command line.

```
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
# echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

Managing Address Pools for Solaris IP Filter

Use the following procedures to manage, view, and modify address pools.

▼ How to View Active Address Pools

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **View the active address pool.**

```
# ippool -l
```

Example 25-12 Viewing the Active Address Pool

The following example shows how to view the contents of the active address pool.

```
# ippool -l
table role = ipf type = tree number = 13
    { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

▼ How to Remove an Address Pool

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Remove the entries in the current address pool.**

```
# ippool -F
```

Example 25-13 Removing an Address Pool

The following example shows how to remove an address pool.

```
# ippool -l
table role = ipf type = tree number = 13
    { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# ippool -F
1 object flushed
# ippool -l
```

▼ How to Append Rules to an Address Pool

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Use one of the following methods to append rules to the active rule set:**

- Append rules to the rule set at the command line using the `ippool -f -` command.

```
# echo "table role = ipf type = tree number = 13
{10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24};" | ippool -f -
```

- Perform the following commands:
 - a. Create additional address pools in a file of your choice.
 - b. Add the rules you have created to the active address pool.

```
# ippool -f filename
```

The rules in *filename* are added to the end of the active address pool.

Example 25-14 Appending Rules to an Address Pool

The following example shows how to add an address pool to the address pool rule set from the command line.

```
# ippool -l
table role = ipf type = tree number = 13
    { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# echo "table role = ipf type = tree number = 100
{10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24};" | ippool -f -
# ippool -l
table role = ipf type = tree number = 100
    { 10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24; };
table role = ipf type = tree number = 13
    { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

Displaying Statistics and Information for Solaris IP Filter

TABLE 25-4 Displaying Solaris IP Filter Statistics and Information (Task Map)

Task	Description	For Instructions
View state tables.	View state tables to obtain information on packet filtering using the <code>ipfstat</code> command.	“How to View State Tables for Solaris IP Filter” on page 566
View state statistics.	View statistics on packet state information using the <code>ipfstat -s</code> command.	“How to View State Statistics for Solaris IP Filter” on page 567
View NAT statistics.	View NAT statistics using the <code>ipnat -s</code> command.	“How to View NAT Statistics for Solaris IP Filter” on page 567

TABLE 25-4 Displaying Solaris IP Filter Statistics and Information (Task Map) *(Continued)*

Task	Description	For Instructions
View address pool statistics.	View address pool statistics using the <code>ippool -s</code> command.	“How to View Address Pool Statistics for Solaris IP Filter” on page 568
View <code>pfil</code> statistics.	View statistics for the <code>pfil</code> module to help you troubleshoot Solaris IP Filter using the <code>ndd</code> command.	“How to View <code>pfil</code> Statistics for Solaris IP Filter” on page 568

▼ How to View State Tables for Solaris IP Filter

- Steps** 1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see *“Configuring RBAC (Task Map)”* in *System Administration Guide: Security Services*.

2. **View the state table.**

```
# ipfstat
```

Note – You can use the `-t` option to view the state table in the top utility format.

Example 25-15 Viewing State Tables for Solaris IP Filter

The following example shows how to view a state table.

```
# ipfstat
bad packets:          in 0    out 0
input packets:       blocked 160 passed 11 nomatch 1 counted 0 short 0
output packets:      blocked 0 passed 13681 nomatch 6844 counted 0 short 0
input packets logged: blocked 0 passed 0
output packets logged: blocked 0 passed 0
packets logged:      input 0 output 0
log failures:        input 0 output 0
fragment state(in):  kept 0 lost 0
fragment state(out): kept 0 lost 0
packet state(in):    kept 0 lost 0
packet state(out):   kept 0 lost 0
ICMP replies:        0      TCP RSTs sent: 0
Invalid source(in):  0
Result cache hits(in): 152    (out): 6837
IN Pullups succeeded: 0      failed: 0
OUT Pullups succeeded: 0     failed: 0
```

```
Fastroute successes: 0          failures: 0
TCP cksum fails(in): 0          (out): 0
IPF Ticks:          14341469
Packet log flags set: (0)
                    none
```

▼ How to View State Statistics for Solaris IP Filter

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**
You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **View the state statistics.**

```
# ipfstat -s
```

Example Viewing State Statistics for Solaris IP Filter 25–16

The following example shows how to view state statistics.

```
# ipfstat -s
IP states added:
  0 TCP
  0 UDP
  0 ICMP
  0 hits
  0 misses
  0 maximum
  0 no memory
  0 max bucket
  0 active
  0 expired
  0 closed
State logging enabled

State table bucket statistics:
  0 in use
  0.00% bucket usage
  0 minimal length
  0 maximal length
  0.000 average length
```

▼ How to View NAT Statistics for Solaris IP Filter

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. View NAT statistics.

```
# ipnat -s
```

Example 25-17 Viewing NAT Statistics for Solaris IP Filter

The following example shows how to view NAT statistics.

```
# ipnat -s
mapped in      0      out      0
added  0      expired 0
no memory      0      bad nat 0
inuse  0
rules  1
wilds  0
```

▼ How to View Address Pool Statistics for Solaris IP Filter

Steps 1. Assume a role that includes the IP Filter Management rights profile, or become superuser.

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. View address pool statistics.

```
# ippool -s
```

Example 25-18 Viewing Address Pool Statistics for Solaris IP Filter

The following example shows how to view address pool statistics.

```
# ippool -s
Pools: 3
Hash Tables: 0
Nodes: 0
```

▼ How to View `pfil` Statistics for Solaris IP Filter

You can view `pfil` statistics when you are troubleshooting Solaris IP Filter.

- Steps** 1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**
- You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **View `pfil` statistics.**

```
# ndd -get /dev/pfil qif_status
```

Example 25-19 Viewing `pfil` Statistics for Solaris IP Filter

The following example shows how to view `pfil` statistics.

```
# ndd -get /dev/pfil qif_status
ifname ill q OTHERQ num sap hl nr nw bad copy copyfail drop notip nodata
notdata
QIP6 0 300011247b8 300011248b0 6 806 0 4 9 0 0 0 0 0 0 0
dmfe1 3000200a018 30002162a50 30002162b48 5 800 14 171 13681 0 0 0 0 0 0 0
```

Working With Log Files for Solaris IP Filter

TABLE 25-5 Working With Solaris IP Filter Log Files (Task Map)

Task	Description	For Instructions
View log files.	View state, NAT, and normal log files using the <code>ipmon</code> command.	“How to View Solaris IP Filter Log Files” on page 569
Flush the packet log buffer.	Remove the contents of the packet log buffer using the <code>ipmon -F</code> command.	“How to Flush the Packet Log File” on page 570
Save logged packets to a file.	Save logged packets to a file for later reference.	“How to Save Logged Packets to a File” on page 571

▼ How to View Solaris IP Filter Log Files

- Steps** 1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**
- You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in

System Administration Guide: Security Services.

2. **View the state, NAT, or normal log files. To view a log file, type one of the following commands, using the appropriate option:**

```
# ipmon -o [S|N|I] filename
```

```
# ipmon -a
```

```
# ipmon -a filename
```

Including the *filename* variable writes the log output to the *filename* file.

S Displays the state log file.

N Displays the NAT log file.

I Displays the normal IP log file.

-a Displays all state, NAT, and normal log files.

For more information on viewing log files, see the `ipmon(1M)` man page.

Example 25-20 Viewing Solaris IP Filter Log Files

The following example shows the output from a log file.

```
# ipmon -a
02/09/2004 15:27:20.606626 hme0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

▼ How to Flush the Packet Log File

- Steps**
1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Flush the pack log buffer.**

```
# ipmon -F
```

Example 25-21 Flushing the Packet Log File

The following example shows the output when a log file is removed. The system provides a report even when there is nothing stored in the log file, as in this example.

```
# ipmon -F
0 bytes flushed from log buffer
0 bytes flushed from log buffer
```

0 bytes flushed from log buffer

▼ How to Save Logged Packets to a File

- Steps** 1. Assume a role that includes the IP Filter Management rights profile, or become superuser.

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. Save the logged packets to a file.

```
# cat /dev/ipl > filename
```

Continue logging packets to the *filename* file until you interrupt the procedure by typing Control-C to get the command line prompt back.

Example 25-22 Saving Logged Packets to a File

The following example shows the result when logged packets are saved to a file.

```
# cat /dev/ipl > /tmp/logfile
^C#

# ipmon -f /tmp/logfile
02/09/2004 15:30:28.708294 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 52 -S IN
02/09/2004 15:30:28.708708 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.792611 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 70 -AP IN
02/09/2004 15:30:28.872000 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872142 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 43 -AP IN
02/09/2004 15:30:28.872808 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872951 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 47 -AP IN
02/09/2004 15:30:28.926792 hme0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 40 -A IN
.
.
(output truncated)
```

Creating and Editing Solaris IP Filter Configuration Files

You must directly edit the configuration files to create and modify rule sets and address pools. Configuration files follow standard UNIX syntax rules:

- The pound sign (#) indicates a line containing comments.
- Rules and comments can coexist on the same line.
- Extraneous white space is allowed to keep rules easy to read.
- Rules can be more than one line long. Use the backslash (\) at the end of a line to indicate that the rule continues on the next line.

▼ How to Create a Configuration File for Solaris IP Filter

The following procedure describes how to set up the following:

- Packet filtering configuration files
- NAT rules configuration files
- Address pool configuration files

Steps 1. **Assume a role that includes the IP Filter Management rights profile, or become superuser.**

You can assign the IP Filter Management rights profile to a role that you create. To create the role and assign the role to a user, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Start the file editor of your choice. Create or edit the configuration file for the feature you want to configure.**

- To create a configuration file for packet filtering rules, edit the `ipf.conf` file. Solaris IP Filter uses the packet filtering rules that you put in to the `ipf.conf` file. If you locate the rules file for packet filtering in the `/etc/ipf/ipf.conf` file, this file is loaded when the system is booted. If you do not want the filtering rules to be loaded at boot time, put the `ipf.conf` file in a location of your choice. You can then activate the rules with the `ipf` command, as described in “How to Activate a Different Packet Filtering Rule Set” on page 556.

See “Using Solaris IP Filter’s Packet Filtering Feature” on page 537 for information on creating packet filtering rules.

Note – If the `ipf.conf` file is empty, there is no filtering. An empty `ipf.conf` file is the same as having a rule set that reads:

```
pass in all
pass out all
```

- To create a configuration file for NAT rules, edit the `ipnat.conf` file.
Solaris IP Filter uses the NAT rules that you put in to the `ipnat.conf` file. If you locate the rules file for NAT in the `/etc/ipf/ipnat.conf` file, this file is loaded when the system is booted. If you do not want the NAT rules loaded at boot time, put the `ipnat.conf` file in a location of your choice. You can then activate the NAT rules with the `ipnat` command.
See [“Using Solaris IP Filter’s NAT Feature” on page 540](#) for information on creating rules for NAT.
- To create a configuration file for address pools, edit the `ippool.conf` file.
Solaris IP Filter uses the pool of addresses that you put in to the `ippool.conf` file. If you locate the rules file for the pool of addresses in the `/etc/ipf/ippool.conf` file, this file is loaded when the system is booted. If you do not want the pool of addresses loaded at boot time, put the `ippool.conf` file in a location of your choice. You can then activate the pool of addresses with the `ippool` command.
See [“Using Solaris IP Filter’s Address Pools Feature” on page 541](#) for information on creating address pools.

Solaris IP Filter Configuration File Examples

The following examples provide an illustration of packet filtering rules used in filtering configurations.

EXAMPLE 25–23 Solaris IP Filter Host Configuration

This example shows a configuration on a host machine with an `elx1` network interface.

```
# pass and log everything by default
pass in log on elx10 all
pass out log on elx10 all

# block, but don't log, incoming packets from other reserved addresses
block in quick on elx10 from 10.0.0.0/8 to any
block in quick on elx10 from 172.16.0.0/12 to any

# block and log untrusted internal IPs. 0/32 is notation that replaces
```

EXAMPLE 25-23 Solaris IP Filter Host Configuration (Continued)

```
# address of the machine running Solaris IP Filter.
block in log quick from 192.168.1.15 to 0/32
block in log quick from 192.168.1.43 to 0/32

# block and log X11 (port 6000) and remote procedure call and portmapper (port 111) attempts
block in log quick on elx10 proto tcp from any to 0/32 port = 6000 keep state
block in log quick on elx10 proto tcp/udp from any to 0/32 port = 111 keep state
```

This rule set begins with two unrestricted rules that allow everything to pass into and out of the `elx1` interface. The second set of rules blocks any incoming packets from the private address spaces `10.0.0.0` and `172.16.0.0` from entering the firewall. The next set of rules blocks specific internal addresses from the host machine. Finally, the last set of rules blocks packets coming in on port 6000 and port 111.

EXAMPLE 25-24 Solaris IP Filter Server Configuration

This example shows a configuration for a host machine acting as a web server. This machine has an `eri` network interface.

```
# web server with an eri interface
# block and log everything by default; then allow specific services
# group 100 - inbound rules
# group 200 - outbound rules
# (0/32) resolves to our IP address)
*** FTP proxy ***

# block short packets which are packets fragmented too short to be real.
block in log quick all with short

# block and log inbound and outbound by default, group by destination
block in log on eri0 from any to any head 100
block out log on eri0 from any to any head 200

# web rules that get hit most often
pass in quick on eri0 proto tcp from any to 0/32 port = http flags S keep state group 100
pass in quick on eri0 proto tcp from any to 0/32 port = https flags S keep state group 100

# inbound traffic - ssh, auth
pass in quick on eri0 proto tcp from any to 0/32 port = 22 flags S keep state group 100
pass in log quick on eri0 proto tcp from any to 0/32 port = 113 flags S keep state group 100
pass in log quick on eri0 proto tcp from any port = 113 to 0/32 flags S keep state group 100

# outbound traffic - DNS, auth, NTP, ssh, WWW, smtp
pass out quick on eri0 proto tcp/udp from 0/32 to any port = domain flags S keep state
group 200
```

EXAMPLE 25–24 Solaris IP Filter Server Configuration (Continued)

```
pass in quick on eri0 proto udp from any port = domain to 0/32 group 100

pass out quick on eri0 proto tcp from 0/32 to any port = 113 flags S keep state group 200
pass out quick on eri0 proto tcp from 0/32 port = 113 to any flags S keep state group 200

pass out quick on eri0 proto udp from 0/32 to any port = ntp group 200
pass in quick on eri0 proto udp from any port = ntp to 0/32 port = ntp group 100

pass out quick on eri0 proto tcp from 0/32 to any port = ssh flags S keep state group 200

pass out quick on eri0 proto tcp from 0/32 to any port = http flags S keep state group 200
pass out quick on eri0 proto tcp from 0/32 to any port = https flags S keep state group 200

pass out quick on eri0 proto tcp from 0/32 to any port = smtp flags S keep state group 200

# pass icmp packets in and out
pass in quick on eri0 proto icmp from any to 0/32 keep state group 100
pass out quick on eri0 proto icmp from 0/32 to any keep state group 200

# block and ignore NETBIOS packets
block in quick on eri0 proto tcp from any to any port = 135 flags S keep state group 100

block in quick on eri0 proto tcp from any port = 137 to any flags S keep state group 100
block in quick on eri0 proto udp from any to any port = 137 group 100
block in quick on eri0 proto udp from any port = 137 to any group 100

block in quick on eri0 proto tcp from any port = 138 to any flags S keep state group 100
block in quick on eri0 proto udp from any port = 138 to any group 100

block in quick on eri0 proto tcp from any port = 139 to any flags S keep state
group 100
block in quick on eri0 proto udp from any port = 139 to any group 100
```

EXAMPLE 25–25 Solaris IP Filter Router Configuration

This example shows a configuration for a router that has an internal interface, ce0, and an external interface, ce1.

```
# internal interface is ce0 at 192.168.1.1
# external interface is ce1 IP obtained via DHCP
# block all packets and allow specific services
*** NAT ***
*** POOLS ***

# Short packets which are fragmented too short to be real.
block in log quick all with short
```

EXAMPLE 25-25 Solaris IP Filter Router Configuration (Continued)

```
# By default, block and log everything.
block in log on ce0 all
block in log on ce1 all
block out log on ce0 all
block out log on ce1 all

# Packets going in/out of network interfaces that aren't on the loopback
# interface should not exist.
block in log quick on ce0 from 127.0.0.0/8 to any
block in log quick on ce0 from any to 127.0.0.0/8
block in log quick on ce1 from 127.0.0.0/8 to any
block in log quick on ce1 from any to 127.0.0.0/8

# Deny reserved addresses.
block in quick on ce1 from 10.0.0.0/8 to any
block in quick on ce1 from 172.16.0.0/12 to any
block in log quick on ce1 from 192.168.1.0/24 to any
block in quick on ce1 from 192.168.0.0/16 to any

# Allow internal traffic
pass in quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24
pass out quick on ce0 from 192.168.1.0/24 to 192.168.1.0/24

# Allow outgoing DNS requests from our servers on .1, .2, and .3
pass out quick on ce1 proto tcp/udp from 0/32 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.2 to any port = domain keep state
pass in quick on ce0 proto tcp/udp from 192.168.1.3 to any port = domain keep state

# Allow NTP from any internal hosts to any external NTP server.
pass in quick on ce0 proto udp from 192.168.1.0/24 to any port = 123 keep state
pass out quick on ce1 proto udp from any to any port = 123 keep state

# Allow incoming mail
pass in quick on ce1 proto tcp from any to 0/32 port = smtp keep state
pass in quick on ce1 proto tcp from any to 0/32 port = smtp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = smtp keep state

# Allow outgoing connections: SSH, WWW, NNTP, mail, whois
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 22 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 22 keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 80 keep state
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = 443 keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = 443 keep state
```


EXAMPLE 25–25 Solaris IP Filter Router Configuration (Continued)

```
pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = nntp keep state
block in quick on ce1 proto tcp from any to any port = nntp keep state
pass out quick on ce1 proto tcp from 192.168.1.0/24 to any port = nntp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = smtp keep state

pass in quick on ce0 proto tcp from 192.168.1.0/24 to any port = whois keep state
pass out quick on ce1 proto tcp from any to any port = whois keep state

# Allow ssh from offsite
pass in quick on ce1 proto tcp from any to 0/32 port = 22 keep state

# Allow ping out
pass in quick on ce0 proto icmp all keep state
pass out quick on ce1 proto icmp all keep state

# allow auth out
pass out quick on ce1 proto tcp from 0/32 to any port = 113 keep state
pass out quick on ce1 proto tcp from 0/32 port = 113 to any keep state

# return rst for incoming auth
block return-rst in quick on ce1 proto tcp from any to any port = 113 flags S/SA

# log and return reset for any TCP packets with S/SA
block return-rst in log on ce1 proto tcp from any to any flags S/SA

# return ICMP error packets for invalid UDP packets
block return-icmp(net-unr) in proto udp all
```


PART **V** Mobile IP

This part introduces Mobile Internet Protocol (Mobile IP) and contains tasks for Mobile IP administration. You can install Mobile IP on systems such as laptops and wireless communications, enabling these computers to operate on foreign networks.

Mobile IP (Overview)

Mobile Internet Protocol (IP) enables the transfer of information between mobile computers. *Mobile computers* include lap tops and wireless communications. The mobile computer can change its location to a foreign network. At the foreign network, the mobile computer can still communicate through the home network of the mobile computer. The Solaris implementation of Mobile IP supports only IPv4.

This chapter contains the following information:

- “Introduction to Mobile IP” on page 581
- “Mobile IP Functional Entities” on page 583
- “How Mobile IP Works” on page 584
- “Agent Discovery” on page 587
- “Care-of Addresses” on page 588
- “Mobile IP With Reverse Tunneling” on page 589
- “Mobile IP Registration” on page 591
- “Routing Datagrams to and From Mobile Nodes” on page 595
- “Security Considerations for Mobile IP” on page 597

For Mobile IP-related tasks, refer to [Chapter 27](#). For Mobile IP reference materials, refer to [Chapter 28](#).

Introduction to Mobile IP

Current versions of the Internet Protocol (IP) assume that the point at which a computer attaches to the Internet or a network is fixed. IP also assumes that the IP address of the computer identifies the network to which the computer is attached. Datagrams that are sent to a computer are based on the location information that is

contained in the IP address. Many Internet Protocols require that a node's IP address remain unchanged. If any of these protocols are active on a Mobile IP computing device, their applications fail. Even HTTP would fail if not for the short-lived nature of its TCP connections. Updating an IP address and refreshing the web page is not a burden.

If a mobile computer, or *mobile node*, moves to a new network while its IP address is unchanged, the mobile node address does not reflect the new point of attachment. Consequently, routing protocols that exist cannot route datagrams to the mobile node correctly. You must reconfigure the mobile node with a different IP address that represents the new location. Assigning a different IP address is cumbersome. Thus, under the current Internet Protocol, if the mobile node moves without changing its address, it loses routing. If the mobile node does change its address, it loses connections.

Mobile IP solves this problem by allowing the mobile node to use two IP addresses. The first address is a fixed *home address*. The second address is a *care-of address* that changes at each new point of attachment. Mobile IP enables a computer to roam freely on the Internet. Mobile IP also enables a computer to roam freely on an organization's network while still maintaining the same home address. Consequently, communication activities are not disrupted when the user changes the computer's point of attachment. Instead, the network is updated with the new location of the mobile node. See the [Glossary](#) for definitions of terms that are associated with Mobile IP.

The following figure illustrates the general Mobile IP topology.

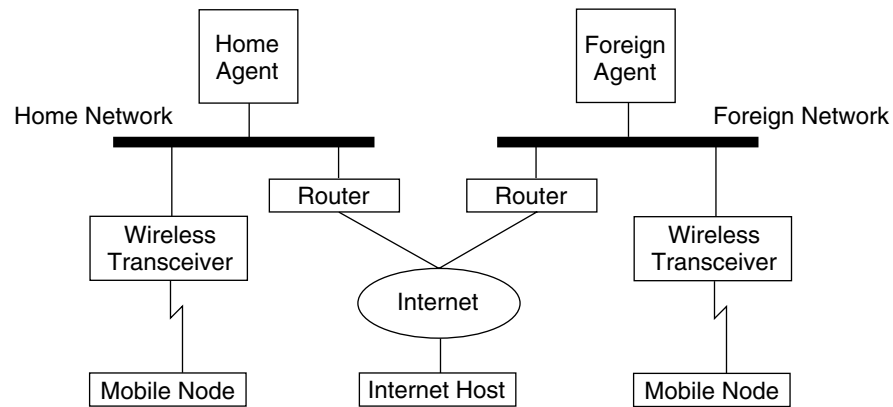


FIGURE 26-1 Mobile IP Topology

By using this figure's Mobile IP topology, the following scenario shows how a datagram moves from one point to another point within the Mobile IP framework:

1. The Internet host sends a datagram to the mobile node by using the mobile node's home address (normal IP routing process).

2. If the mobile node is on its home network, the datagram is delivered through the normal IP process to the mobile node. Otherwise, the home agent receives the datagram.
3. If the mobile node is on a foreign network, the home agent forwards the datagram to the foreign agent. The home agent must encapsulate the datagram in an outer datagram so that the foreign agent's IP address appears in the outer IP header.
4. The foreign agent delivers the datagram to the mobile node.
5. Datagrams from the mobile node to the Internet host are sent by using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The foreign agent forwards the datagram to the Internet host.
6. In situations with ingress filtering present, the source address must be topologically correct for the subnet that the datagram is coming from, or a router cannot forward the datagram. If this scenario exists on links between the mobile node and the correspondent node, the foreign agent needs to provide reverse tunneling support. Then, the foreign agent can deliver every datagram that the mobile node sends to its home agent. The home agent then forwards the datagram through the path that the datagram would have taken had the mobile node resided on the home network. This process guarantees that the source address is correct for all links that the datagram must traverse.

Regarding wireless communications, [Figure 26-1](#) depicts the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the mobile node use the home address of the mobile node. The home address is used even when the mobile node is located on the foreign network. The care-of address is used only for communication with mobility agents. The care-of address is invisible to the Internet host.

Mobile IP Functional Entities

Mobile IP introduces the following new functional entities:

- **Mobile node (MN)** – Host or router that changes its point of attachment from one network to another network while maintaining all existing communications by using its IP home address.
- **Home agent (HA)** – Router or server on the home network of a mobile node. The router intercepts datagrams that are destined for the mobile node. The router then delivers the datagrams through the care-of address. The home agent also maintains current information on the location of the mobile node.
- **Foreign agent (FA)** – Router or server on the foreign network that the mobile node visits. Provides host routing services to the mobile node. The foreign agent might also provide a care-of address to the mobile node while the mobile node is registered.

How Mobile IP Works

Mobile IP enables routing of IP datagrams to mobile nodes. The home address of the mobile node always identifies the mobile node regardless of where the mobile node is attached. When away from home, a care-of address is associated with the mobile node's home address. The care-of address provides information about the current point of attachment of the mobile node. Mobile IP uses a registration mechanism to register the care-of address with a home agent.

The home agent redirects datagrams from the home network to the care-of address. The home agent constructs a new IP header that contains the care-of address of the mobile node as the destination IP address. This new header encapsulates the original IP datagram. Consequently, the home address of the mobile node has no effect on the routing of the encapsulated datagram until the datagram arrives at the care-of address. This type of encapsulation is called *tunneling*. After the datagram arrives at the care-of address, the datagram is de-encapsulated. Then the datagram is delivered to the mobile node.

The following figure shows a mobile node that resides on its home network, Network A, before the mobile node moves to a foreign network, Network B. Both networks support Mobile IP. The mobile node is always associated with the home address of the mobile node, 128.226.3.30.

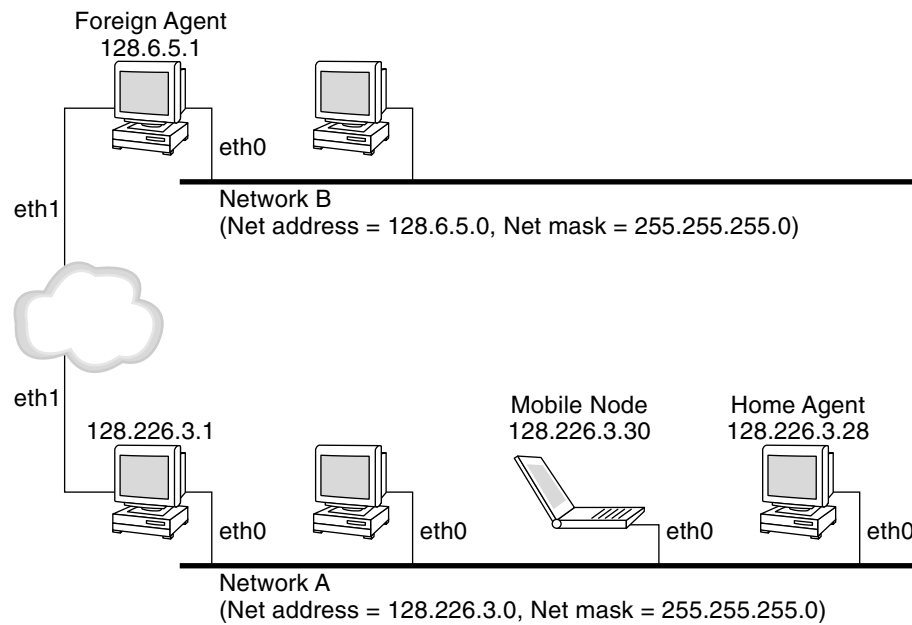


FIGURE 26-2 Mobile Node Residing on Home Network

The following figure shows a mobile node that has moved to a foreign network, Network B. Datagrams that are destined for the mobile node are intercepted by the home agent on the home network, Network A. The datagrams are encapsulated. Then, the datagrams are sent to the foreign agent on Network B. The foreign agent strips off the outer header. Then the foreign agent delivers the datagram to the mobile node that is located on Network B.

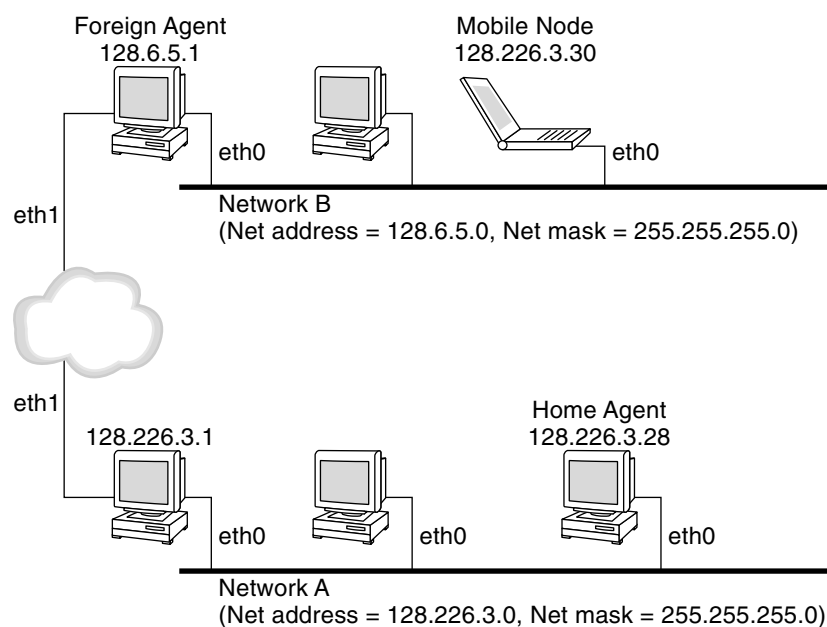


FIGURE 26-3 Mobile Node Moving to a Foreign Network

The care-of address might belong to a foreign agent. The care-of address might be acquired by the mobile node through the Dynamic Host Configuration Protocol (DHCP) or the Point-to-Point Protocol (PPP). In the latter situation, a mobile node has a colocated care-of address.

Mobility agents (home agents and foreign agents) advertise their presence by using *agent advertisement* messages. Optionally, a mobile node can solicit an agent advertisement message. The mobile node uses any mobility agent that is attached locally through an *agent solicitation* message. A mobile node uses the agent advertisements to determine whether the mobile node is on the home network or a foreign network.

The mobile node uses a special registration process to inform the home agent about the current location of the mobile node. The mobile node is always “listening” for mobility agents advertising their presence. The mobile node uses these advertisements to help determine when the mobile node moves to another subnet. When a mobile node determines that the mobile node has moved its location, the mobile node uses the new foreign agent to forward a registration message to the home agent. The mobile node uses the same process when the mobile node moves from one foreign network to another foreign network.

When the mobile node detects that it is located on the home network, the mobile node does not use mobility services. When the mobile node returns to the home network, the mobile node *deregisters* with the home agent.

Agent Discovery

A mobile node uses a method that is known as *agent discovery* to determine the following information:

- When the node has moved from one network to another network
- Whether the network is the home network or a foreign network
- The foreign agent care-of address that is offered by each foreign agent on that network
- Mobility services that are provided by the mobility agent, advertised as flags, and additional extensions in the agent advertisement

Mobility agents transmit *agent advertisements* to advertise services on a network. In the absence of agent advertisements, a mobile node can solicit advertisements. This capability is known as *agent solicitation*. If a mobile node is capable of supporting its own colocated care-of address, the mobile node can use regular router advertisements for the same purposes.

Agent Advertisement

Mobile nodes use agent advertisements to determine the current point of attachment to the Internet or to an organization's network. An agent advertisement is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension.

A foreign agent (FA) can be too busy to serve additional mobile nodes. However, a foreign agent must continue to send agent advertisements. Then, the mobile node, which is already registered with a foreign agent, knows that the mobile node has not moved out of range of the foreign agent. The mobile node also knows that the foreign agent has not failed. A mobile node that is registered with a foreign agent from which it no longer receives agent advertisements probably knows that the mobile node can no longer contact that foreign agent.

Agent Advertisement Over Dynamic Interfaces

You can configure the implementation of the foreign agent to send advertisements over dynamically created interfaces. You have options to enable or disable limited unsolicited advertisements over the advertising interfaces. Dynamically created interfaces are defined as only those interfaces that are configured after the `mipagent` daemon starts. Advertisement over dynamic interfaces is useful for applications that support transient mobility interfaces. Moreover, by limiting unsolicited advertisement, network bandwidth might be saved.

Agent Solicitation

Every mobile node should implement agent solicitation. The mobile node uses the same procedures, defaults, and constants for agent solicitation that are specified for solicitation messages of ICMP routers.

The rate that a mobile node sends solicitations is limited by the mobile node. The mobile node can send three initial solicitations at a maximum rate of one solicitation per second while the mobile node searches for an agent. After the mobile node registers with an agent, the rate that solicitations are sent is reduced to limit the overhead on the local network.

Care-of Addresses

Mobile IP provides the following alternative modes for the acquisition of a care-of address:

- A foreign agent provides a *foreign agent care-of address*, which is advertised to the mobile node through agent advertisement messages. The care-of address is usually the IP address of the foreign agent that sends the advertisements. The foreign agent is the endpoint of the tunnel. When the foreign agent receives datagrams through a tunnel, the foreign agent de-encapsulates the datagrams. Then, the foreign agent delivers the inner datagram to the mobile node. Consequently, many mobile nodes can share the same care-of address. Bandwidth is important on wireless links. Wireless links are good candidates from which foreign agents can provide Mobile IP services to higher bandwidth-wired links.
- A mobile node acquires a *colocated care-of address* as a local IP address through some external means. The mobile node then associates with one of its own network interfaces. The mobile node might acquire the address through DHCP as a temporary address. The address might also be owned by the mobile node as a long-term address. However, the mobile node can only use the address while visiting the subnet to which this care-of address belongs. When using a colocated care-of address, the mobile node serves as the endpoint of the tunnel. The mobile node performs de-encapsulation of the datagrams that are tunneled to the mobile node.

A colocated care-of address enables a mobile node to function without a foreign agent. Consequently, a mobile node can use a colocated care-of address in networks that have not deployed a foreign agent.

If a mobile node is using a colocated care-of address, the mobile node must be located on the link that is identified by the network prefix of the care-of address. Otherwise, datagrams that are destined to the care-of address cannot be delivered.

Mobile IP With Reverse Tunneling

The section “[How Mobile IP Works](#)” on page 584 assumes that the routing within the Internet is independent of the source address of the datagram. However, intermediate routers might check for a topologically correct source address. If an intermediate router does check, the mobile node needs to set up a reverse tunnel. By setting up a reverse tunnel from the care-of address to the home agent, you ensure a topologically correct source address for the IP data packet. Reverse tunnel support is advertised by foreign agents and home agents. A mobile node can request a reverse tunnel between the foreign agent and the home agent when the mobile node registers. A reverse tunnel is a tunnel that starts at the care-of address of the mobile node and terminates at the home agent. The following figure shows the Mobile IP topology that uses a reverse tunnel.

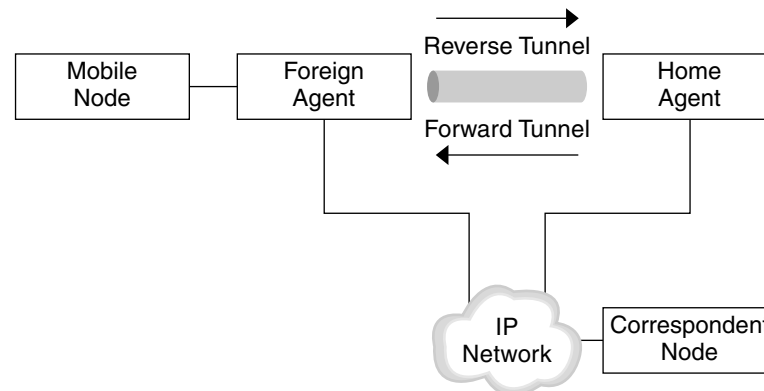


FIGURE 26-4 Mobile IP With a Reverse Tunnel

Limited Private Addresses Support

Mobile nodes that have private addresses that are not globally routeable through the Internet require reverse tunnels. Solaris Mobile IP supports mobile nodes that are privately addressed. See “[Overview of the Solaris Mobile IP Implementation](#)” on page 615 for the functions that Solaris Mobile IP does not support.

Enterprises employ private addresses when external connectivity is not required. Private addresses are not routeable through the Internet. When a mobile node has a private address, the mobile node can only communicate with a correspondent node by having its datagrams reverse-tunneled to its home agent. The home agent then

delivers the datagram to the correspondent node in whatever manner the datagram is normally delivered when the mobile node is at home. The following figure shows a network topology with two mobile nodes that are privately addressed. The two mobile nodes use the same care-of address when they are registered to the same foreign agent.

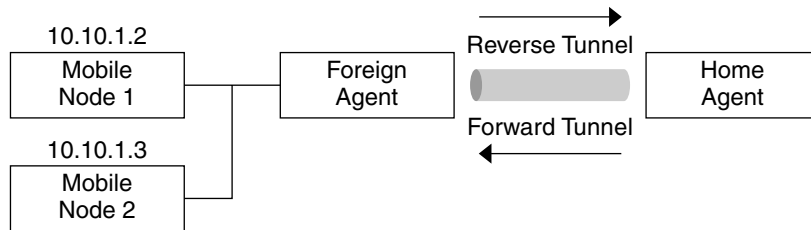


FIGURE 26-5 Privately Addressed Mobile Nodes Residing on the Same Foreign Network

The care-of address and the home agent address must be globally routable addresses if these addresses belong to different domains that are connected by a public Internet.

The same foreign network can include two mobile nodes that are privately addressed with the same IP address. However, each mobile node must have a different home agent. Also, each mobile node must be on different advertising subnets of a single foreign agent. The following figure shows a network topology that depicts this situation.

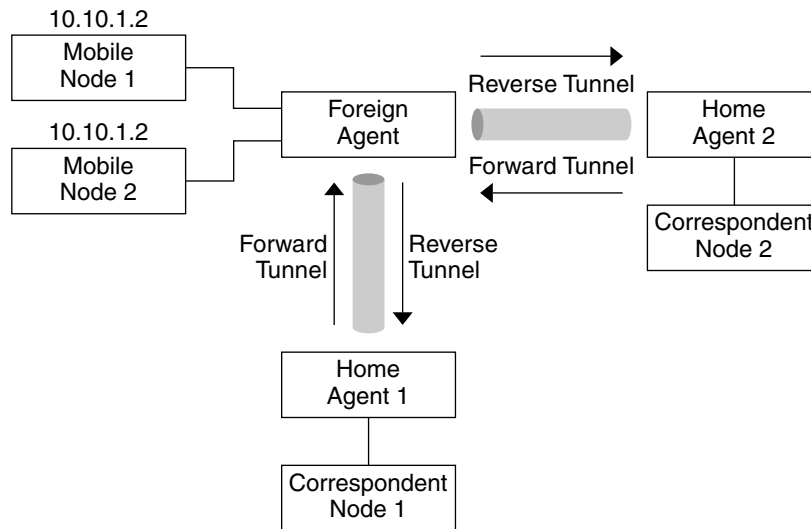


FIGURE 26-6 Privately Addressed Mobile Nodes Residing on Different Foreign Networks

Mobile IP Registration

Mobile nodes detect when they have moved from one subnet to another subnet through the use of agent advertisements. When the mobile node receives an agent advertisement that indicates that the mobile node has changed locations, the mobile node registers through a foreign agent. Even though the mobile node might have acquired its own colocated care-of address, this feature is provided to enable sites to restrict access to mobility services.

Mobile IP registration provides a flexible mechanism for mobile nodes to communicate the current reachability information to the home agent. The registration process enables mobile nodes to perform the following tasks:

- Request forwarding services when visiting a foreign network
- Inform the home agent of the current care-of address
- Renew a registration that is about to expire
- Deregister when the mobile node returns home
- Request a reverse tunnel

Registration messages exchange information between a mobile node, a foreign agent, and the home agent. Registration creates or modifies a mobility binding at the home agent. Registration associates the home address of the mobile node with the care-of address of the mobile node for the specified lifetime.

The registration process also enables mobile nodes to do the following functions:

- Register with multiple foreign agents
- Deregister specific care-of addresses while retaining other mobility bindings
- Discover the address of a home agent if the mobile node is not configured with this information

Mobile IP defines the following registration processes for a mobile node:

- If a mobile node registers a foreign agent care-of address, the mobile node is informing the home agent that it is reachable through that foreign agent.
- If a mobile node receives an agent advertisement that requires the mobile node to register through a foreign agent, the mobile node can still attempt to obtain a colocated care-of address. The mobile node can also register with that foreign agent or any other foreign agent on that link.
- If a mobile node uses a colocated care-of address, the mobile node registers directly with the home agent.
- If a mobile node returns to the home network, the mobile node deregisters with the home agent.

These registration processes involve the exchange of registration requests and registration reply messages. When the mobile node registers by using a foreign agent, the registration process takes the following steps, which the subsequent figure shows:

1. The mobile node sends a registration request to the prospective foreign agent to begin the registration process.
2. The foreign agent processes the registration request and then relays the request to the home agent.
3. The home agent sends a registration reply to the foreign agent to grant or deny the request.
4. The foreign agent processes the registration reply and then relays the reply to the mobile node to inform the mobile node of the disposition of the request.

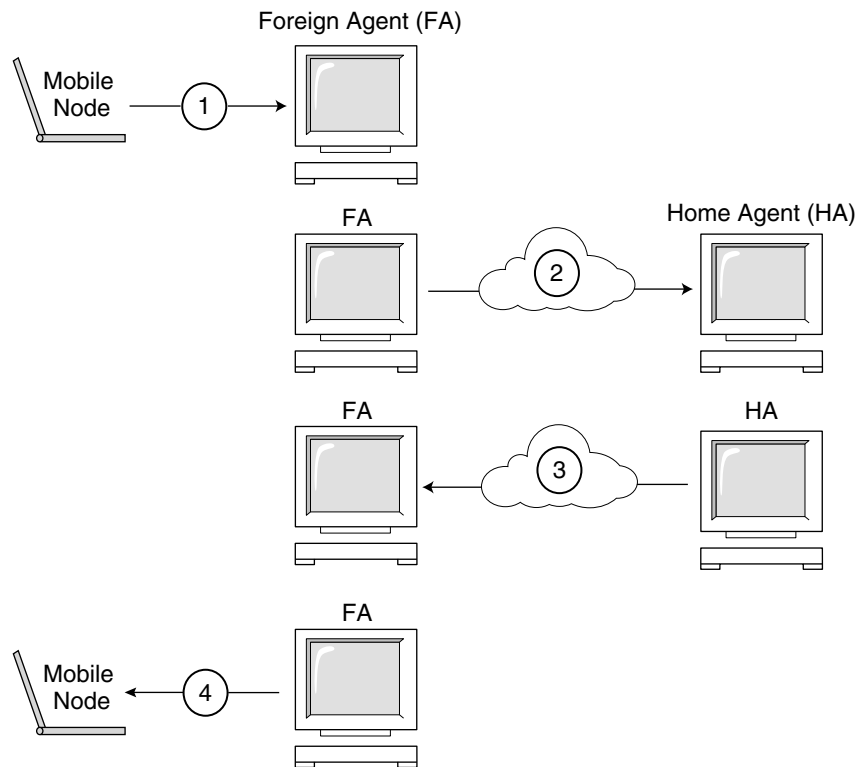


FIGURE 26-7 Mobile IP Registration Process

When the mobile node registers directly with the home agent, the registration process requires only the following steps:

- The mobile node sends a registration request to the home agent.
- The home agent sends a registration reply to the mobile node that grants or denies the request.

Also, either the foreign agent or the home agent might require a reverse tunnel. If the foreign agent supports reverse tunneling, the mobile node uses the registration process to request a reverse tunnel. The mobile node sets the reverse tunnel flag in the registration request to request a reverse tunnel.

Network Access Identifier (NAI)

Authentication, authorization, and accounting (AAA) servers, in use within the Internet, provide authentication and authorization services for dialup computers. These services are likely to be equally valuable for mobile nodes that use Mobile IP when the nodes attempt to connect to foreign domains with AAA servers. AAA servers use the Network Access Identifier (NAI) to identify clients. A mobile node can identify itself by including the NAI in the Mobile IP registration request.

Because the NAI is typically used to uniquely identify the mobile node, the home address of the mobile node is not always necessary to provide that function. Thus, a mobile node can authenticate itself. Consequently, a mobile node can be authorized for connection to the foreign domain without even having a home address. To request that a home address be assigned, a message that contains the mobile node NAI extension can set the home address field to zero in the registration request.

Mobile IP Message Authentication

Each mobile node, foreign agent, and home agent supports a mobility security association between the various Mobile IP components. The security association is indexed by the security parameter index (SPI) and IP address. In the instance of the mobile node, this address is the home address of the mobile node. Registration messages between a mobile node and the home agent are authenticated with the mobile-home authentication extension. In addition to mobile-home authentication, which is mandatory, you can use the optional mobile-foreign agent and home-foreign agent authentications.

Mobile Node Registration Request

A mobile node uses a *registration request* message to register with the home agent. Thus, the home agent can create or modify a mobility binding for that mobile node (for example, with a new lifetime). The foreign agent can relay the registration request to the home agent. However, if the mobile node is registering a colocated care-of address, then the mobile node can send the registration request directly to the home agent. If the foreign agent advertises that registration messages must be sent to the foreign agent, then the mobile node must send the registration request to the foreign agent.

Registration Reply Message

A mobility agent returns a *registration reply* message to a mobile node that has sent a registration request message. If the mobile node requests service from a foreign agent, that foreign agent receives the reply from the home agent. Subsequently, the foreign agent relays the reply to the mobile node. The reply message contains the necessary codes to inform the mobile node and the foreign agent about the status of the registration request. The message also contains the lifetime that is granted by the home agent. The lifetime can be smaller than the original request. The registration reply can also contain a dynamic home address assignment.

Foreign Agent Considerations

The foreign agent plays a mostly passive role in Mobile IP registration. The foreign agent adds all mobile nodes that are registered to the visitor table. The foreign agent relays registration requests between mobile nodes and home agents. Also, when the foreign agent provides the care-of address, the foreign agent de-encapsulates datagrams for delivery to the mobile node. The foreign agent also sends periodic agent advertisement messages to advertise the presence of the foreign agent.

If home agents and foreign agents support reverse tunnels, and the mobile node requests a reverse tunnel, the foreign agent then tunnels all the packets from the mobile node to the home agent. The home agent then sends the packets to the correspondent node. This process is the reverse of the home agent tunneling all of the mobile node's packets to the foreign agent for delivery to the mobile node. A foreign agent that supports reverse tunnels advertises that the reverse tunnel is supported for registration. Because of the local policy, the foreign agent can deny a registration request when the reverse tunnel flag is not set. The foreign agent can only distinguish multiple mobile nodes with the same (private) IP address when these mobile nodes are visiting different interfaces on the foreign agent. In the forward tunnel situation, the foreign agent distinguishes between multiple mobile nodes that share the same private addresses by looking at the incoming tunnel interface. The incoming tunnel interface maps to a unique home agent address.

Home Agent Considerations

Home agents play an active role in the registration process. The home agent receives registration requests from the mobile node. The registration request might be relayed by the foreign agent. The home agent updates its record of the mobility bindings for this mobile node. The home agent issues a suitable registration reply in response to each registration request. The home agent also forwards packets to the mobile node when the mobile node is away from the home network.

A home agent might not have to have a physical subnet configured for mobile nodes. However, the home agent must recognize the home address of the mobile node through the `mipagent.conf` file or some other mechanism when the home agent grants registration. For more information about `mipagent.conf`, refer to [“Creating the Mobile IP Configuration File”](#) on page 600.

A home agent can support private addressed mobile nodes by configuring the private addressed mobile nodes in the `mipagent.conf` file. The home addresses that are used by the home agent must be unique.

Dynamic Home Agent Discovery

In some situations, the mobile node might not know the home agent address when the mobile node attempts to register. If the mobile node does not know the home agent address, the mobile node can use dynamic home agent address resolution to learn the address. In this situation, the mobile node sets the home agent field of the registration request to the subnet-directed broadcast address of its home network. Each home agent that receives a registration request with a broadcast destination address rejects the mobile node’s registration by returning a rejection registration reply. By doing so, the mobile node can use the home agent’s unicast IP address that is indicated in the rejection reply when the mobile node next attempts registration.

Routing Datagrams to and From Mobile Nodes

This section describes how mobile nodes, home agents, and foreign agents cooperate to route datagrams for mobile nodes that are connected to a foreign network. See [“Overview of the Solaris Mobile IP Implementation”](#) on page 615 for Mobile IP functions that are supported in the Solaris OS.

Encapsulation Methods

Home agents and foreign agents use one of the available encapsulation methods to support datagrams that use a tunnel. Defined encapsulation methods are IP-in-IP Encapsulation, Minimal Encapsulation, and Generic Routing Encapsulation. Foreign agent and home agent cases, or indirect collocated mobile node and home agent cases, must support the same encapsulation method. All Mobile IP entities are required to support IP-in-IP Encapsulation.

Unicast Datagram Routing

When registered on a foreign network, the mobile node uses the following rules to choose a default router:

- If the mobile node is registered and uses a foreign agent care-of address, the process is straightforward. The mobile node chooses its default router from among the router addresses that are advertised in the ICMP router advertisement portion of that agent advertisement. The mobile node can also consider the IP source address of the agent advertisement as another possible choice for the IP address of a default router.
- The mobile node might be registered directly with the home agent by using a colocated care-of address. Then, the mobile node chooses its default router from among those routers that are advertised in any ICMP router advertisement message that it receives. The network prefix of the chosen default router must match the network prefix of the care-of address of the mobile node that is externally obtained. The address might match the IP source address of the agent advertisement under the network prefix. Then, the mobile node can also consider that IP source address as another possible choice for the IP address of a default router.
- If the mobile node is registered, a foreign agent that supports reverse tunnels routes unicast datagrams from the mobile node to the home agent through the reverse tunnel. If the mobile node is registered with a foreign agent that provides reverse tunnel support, the mobile node must use that foreign agent as its default router.

Broadcast Datagrams

When a home agent receives a broadcast datagram or multicast datagram, the home agent only forwards the datagram to mobile nodes that have specifically requested that they receive them. How the home agent forwards broadcast and multicast datagrams to mobile nodes depends primarily on two factors. Either that mobile node is using a foreign-agent provided care-of address, or the mobile node is using its own colocated care-of address. The former means that the datagram must be double encapsulated. The first IP header identifies the mobile node for which the datagram is to be delivered. This first IP header is not present in the broadcast or multicast datagram. The second IP header identifies the care-of address, and is the usual tunnel header. In the latter instance, the mobile node is decapsulating its own datagrams, and the datagram needs only to be sent through the regular tunnel.

Multicast Datagram Routing

To begin receiving multicast traffic when a mobile node is visiting a foreign subnet, a mobile node can join a multicast group in any of the following ways:

- If the mobile node is using a colocated care-of address, the mobile node can use this address as the source IP address of any Internet Group Management Protocol (IGMP) join messages. However, a multicast router must be present on the visited subnet.
- If the mobile node wants to join the ICMP group from its home subnet, the mobile node must use a reverse tunnel to send IGMP join messages to the home agent. However, the mobile node's home agent must be a multicast router. The home agent then forwards multicast datagrams through the tunnel to the mobile node.
- If the mobile node is using a colocated care-of address, the mobile node can use this address as the source IP address of any IGMP join messages. However, a multicast router must be present on the visited subnet. After the mobile node has joined the group, the mobile node can participate by sending its own multicast packets directly on the visited network.
- Send directly on the visited network.
- Send through a tunnel to the home agent.

Multicast routing depends on the IP source address. A mobile node that is sending a multicast datagram must send the datagram from a valid source address on that link. So a mobile node that is sending multicast datagrams directly on the visited network must use a colocated care-of address as the IP source address. Also, the mobile node must have joined the multicast group that is associated with the address. Similarly, a mobile node that joined a multicast group while on its home subnet before roaming, or joined the multicast group while roaming through a reverse tunnel to its home agent, must use its home address as the IP source address of the multicast datagram. Thus, the mobile node must have these datagrams reverse-tunneled to its home subnet as well, either through itself by using its colocated care-of address, or through a foreign agent reverse tunnel.

While it seems more efficient for a mobile node to always join from the subnet that the mobile node is visiting, it is still a mobile node. Consequently, the mobile node would have to repeat the join every time the mobile node switches subnets. The more efficient way is for the mobile node to join through its home agent, and not have to carry this overhead. Also, multicast sessions might be present that are only available from the home subnet. Other considerations might also force the mobile node to participate in a specific way.

Security Considerations for Mobile IP

In many situations, mobile computers use wireless links to connect to the network. Wireless links are particularly vulnerable to passive eavesdropping, active replay attacks, and other active attacks.

Because Mobile IP recognizes its inability to reduce or eliminate this vulnerability, Mobile IP uses a form of authentication to protect Mobile IP registration messages from these types of attack. The default algorithm that is used is MD5, with a key size

of 128 bits. The default operational mode requires that this 128-bit key precede and succeed the data to be hashed. The foreign agent uses MD5 to support authentication. The foreign agent also uses key sizes of 128 bits or greater, with manual key distribution. Mobile IP can support more authentication algorithms, algorithm modes, key distribution methods, and key sizes.

These methods do prevent Mobile IP registration messages from being altered. However, Mobile IP also uses a form of replay protection to alert Mobile IP entities when they receive duplicates of previous Mobile IP registration messages. If this protection method were not used, the mobile node and its home agent might become unsynchronized when either of them receives a registration message. Hence, Mobile IP updates its state. For example, a home agent receives a duplicate deregistration message while the mobile node is registered through a foreign agent.

Replay protection is ensured either by a method known as *nonces*, or *timestamps*. Nonces and timestamps are exchanged by home agents and mobile nodes within the Mobile IP registration messages. Nonces and timestamps are protected from change by an authentication mechanism. Consequently, if a home agent or mobile node receives a duplicate message, the duplicate message can be thrown away.

The use of tunnels can be a significant vulnerability, especially if registration is not authenticated. Also, the Address Resolution Protocol (ARP) is not authenticated, and can potentially be used to steal another host's traffic.

Use of IPsec With Mobile IP

In general, because home agents and foreign agents are fixed entities, they can use IPsec authentication or encryption to protect both Mobile IP registration messages and forward and reverse tunnel traffic. This process works completely independently of Mobile IP, and only depends on the workstation's ability to perform IPsec functions. Mobile nodes can also use IPsec authentication to protect their registration traffic. If the mobile node registers through a foreign agent, in general the mobile node cannot use IPsec encryption. The reason that the mobile node cannot use IPsec encryption is because the foreign agent must be able to check the information in the registration packet. While IPsec encryption could be used when a foreign agent is not needed, the issue of colocation makes this difficult to achieve. IPsec is an IP-level security relationship. Consequently, a home agent would have to know the mobile node's collocated address without prior information or registration messages. For more information about IPsec, see [Chapter 18](#) or [Chapter 19](#).

Administering Mobile IP (Tasks)

This chapter provides procedures for modifying, adding, deleting, and displaying parameters in the Mobile IP configuration file. This chapter also shows you how to display mobility agent status.

This chapter contains the following information:

- “Creating the Mobile IP Configuration File (Task Map)” on page 599
- “Creating the Mobile IP Configuration File” on page 600
- “Modifying the Mobile IP Configuration File” on page 606
- “Modifying the Mobile IP Configuration File (Task Map)” on page 605
- “Displaying Mobility Agent Status” on page 612
- “Displaying Mobility Routes on a Foreign Agent” on page 614

For an introduction to Mobile IP, refer to [Chapter 26](#). For detailed information about Mobile IP, refer to [Chapter 28](#).

Creating the Mobile IP Configuration File (Task Map)

Task	Description	For Instructions
Create the Mobile IP configuration file.	Involves creating the <code>/etc/inet/mipagent.conf</code> file or copying one of the sample files.	“How to Create the Mobile IP Configuration File” on page 601

Task	Description	For Instructions
Configure the General section.	Involves typing the version number into the General section of the Mobile IP configuration file.	"How to Configure the General Section" on page 602
Configure the Advertisements section.	Involves adding labels and values, or changing them, in the Advertisements section of the Mobile IP configuration file.	"How to Configure the Advertisements Section" on page 602
Configure the GlobalSecurityParameters section.	Involves adding labels and values, or changing them, in the GlobalSecurityParameters section of the Mobile IP configuration file.	"How to Configure the GlobalSecurityParameters Section" on page 602
Configure the Pool section.	Involves adding labels and values, or changing them, in the Pool section of the Mobile IP configuration file.	"How to Configure the Pool Section" on page 603
Configure the SPI section.	Involves adding labels and values, or changing them, in the SPI section of the Mobile IP configuration file.	"How to Configure the SPI Section" on page 603
Configure the Address section.	Involves adding labels and values, or changing them, in the Address section of the Mobile IP configuration file.	"How to Configure the Address Section" on page 603

Creating the Mobile IP Configuration File

This section explains how to plan for Mobile IP and create the `/etc/inet/mipagent.conf` file.

▼ How to Plan for Mobile IP

When you configure the `mipagent.conf` file for the first time, you need to perform the following tasks:

- Steps**
1. Depending on your organization's requirements for its hosts, determine what functionality your Mobile IP agent can provide:

- Foreign agent functionality only
 - Home agent functionality only
 - Both foreign agent and home agent functionality
2. Create the `/etc/inet/mipagent.conf` file and specify the settings you require by using the procedures that are described in this section. You can also copy one of the following files to `/etc/inet/mipagent.conf` and modify it according to your requirements:
 - For foreign agent functionality, copy `/etc/inet/mipagent.conf.fa-sample`.
 - For home agent functionality, copy `/etc/inet/mipagent.conf.ha-sample`.
 - For both foreign agent and home agent functionality, copy `/etc/inet/mipagent.conf-sample`.
 3. You can reboot your system to invoke the boot script that starts the `mipagent` daemon. Or, you can also start `mipagent` by typing the following command:


```
# /etc/inet.d/mipagent start
```

▼ How to Create the Mobile IP Configuration File

- Steps**
1. Assume the Primary Administrator role, or become superuser, on the system where you want to enable Mobile IP.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.
 2. Create the `/etc/inet/mipagent.conf` file by using one of the following options:
 - In the `/etc/inet` directory, create an empty file named `mipagent.conf`.
 - From the following list, copy the sample file that provides the functionality you want for the `/etc/inet/mipagent.conf` file.
 - `/etc/inet/mipagent.conf.fa-sample`
 - `/etc/inet/mipagent.conf.ha-sample`
 - `/etc/inet/mipagent.conf-sample`
 3. Add or change configuration parameters in the `/etc/inet/mipagent.conf` file to conform to your configuration requirements.

The remaining procedures in this section describe the steps to modify sections in `/etc/inet/mipagent.conf`.

▼ How to Configure the General Section

If you copied one of the sample files in the `/etc/inet` directory, you can omit this procedure because the sample file contains this entry. “[General Section](#)” on page 621 provides descriptions of the labels and values that are used in this section.

- Step** ● **Edit the `/etc/inet/mipagent.conf` file and add the following lines:**

```
[General]
    Version = 1.0
```

Note – The `/etc/inet/mipagent.conf` file must contain this entry.

▼ How to Configure the Advertisements Section

“[Advertisements Section](#)” on page 621 provides descriptions of the labels and values that are used in this section.

- Step** ● **Edit the `/etc/inet/mipagent.conf` file and add or change the following lines by using the values that are required for your configuration.**

```
[Advertisements interface]
    HomeAgent = <yes/no>
    ForeignAgent = <yes/no>
    PrefixFlags = <yes/no>
    AdvertiseOnBcast = <yes/no>
    RegLifetime = n
    AdvLifetime = n
    AdvFrequency = n
    ReverseTunnel = <yes/no/FA/HA/both>
    ReverseTunnelRequired = <yes/no/FA/HA>
```

Note – You must include a different `Advertisements` section for each interface on the local host that provides Mobile IP services.

▼ How to Configure the GlobalSecurityParameters Section

“[GlobalSecurityParameters Section](#)” on page 623 provides descriptions of the labels and values that are used in this section.

- Step** ● **Edit the `/etc/inet/mipagent.conf` file and add or change the following lines by using the values that are required for your configuration:**

```
[GlobalSecurityParameters]
MaxClockSkew = n
HA-FAauth = <yes/no>
MN-FAauth = <yes/no>
Challenge = <yes/no>
KeyDistribution = files
```

▼ How to Configure the Pool Section

“Pool Section” on page 624 provides descriptions of the labels and values that are used in this section:

- Steps**
1. **Edit the `/etc/inet/mipagent.conf` file**
 2. **Add or change the following lines by using the values that are required for your configuration:**

```
[Pool pool-identifier]
BaseAddress = IP-address
Size = size
```

▼ How to Configure the SPI Section

“SPI Section” on page 625 provides descriptions of the labels and values that are used in this section.

- Steps**
1. **Edit the `/etc/inet/mipagent.conf` file.**
 2. **Add or change the following lines by using the values that are required for your configuration:**

```
[SPI SPI-identifier]
ReplayMethod = <none/timestamps>
Key = key
```

Note – You must include a different SPI section for each security context that is deployed.

▼ How to Configure the Address Section

“Address Section” on page 626 provides descriptions of the labels and values that are used in this section.

- Steps**
1. Edit the `/etc/inet/mipagent.conf` file.
 2. Add or change the following lines by using the values that are required for your configuration:

- **For a mobile node, use the following:**

```
[Address address]
  Type = node
  SPI = SPI-identifier
```

- **For an agent, use the following:**

```
[Address address]
  Type = agent
  SPI = SPI-identifier
  IPsecRequest = action {properties} [: action {properties}]
  IPsecReply = action {properties} [: action {properties}]
  IPsecTunnel = action {properties} [: action {properties}]
```

where *action* and *{properties}* are any action and associated properties that are defined in the `ipsec(7P)` man page.

Note – The SPI that is configured previously corresponds to the MD5 protection mechanism that is required by RFC 2002. The SPI that is configured previously does not correspond to the SPI that is used by IPsec. For more information about IPsec, see [Chapter 18](#) and [Chapter 19](#). Also see the `ipsec(7P)` man page.

- **For a mobile node that is identified by its NAI, use the following:**

```
[Address NAI]
  Type = Node
  SPI = SPI-identifier
  Pool = pool-identifier
```

- **For a default mobile node, use the following:**

```
[Address Node-Default]
  Type = Node
  SPI = SPI-identifier
  Pool = pool-identifier
```

Modifying the Mobile IP Configuration File (Task Map)

Task	Description	For Instructions
Modify the General section.	Uses the <code>mipagentconfig change</code> command to change the value of a label in the <code>General</code> section of the Mobile IP configuration file.	“How to Modify the General Section” on page 606
Modify the Advertisements section.	Uses the <code>mipagentconfig change</code> command to change the value of a label in the <code>Advertisements</code> section of the Mobile IP configuration file.	“How to Modify the Advertisements Section” on page 606
Modify the GlobalSecurityParameters section.	Uses the <code>mipagentconfig change</code> command to change the value of a label in the <code>GlobalSecurityParameters</code> section of the Mobile IP configuration file.	“How to Modify the GlobalSecurityParameters Section” on page 607
Modify the Pool section.	Uses the <code>mipagentconfig change</code> command to change the value of a label in the <code>Pool</code> section of the Mobile IP configuration file.	“How to Modify the Pool Section” on page 608
Modify the SPI section.	Uses the <code>mipagentconfig change</code> command to change the value of a label in the <code>SPI</code> section of the Mobile IP configuration file.	“How to Modify the SPI Section” on page 608
Modify the Address section.	Uses the <code>mipagentconfig change</code> command to change the value of a label in the <code>Address</code> section of the Mobile IP configuration file.	“How to Modify the Address Section” on page 609
Add or delete parameters.	Uses the <code>mipagentconfig add</code> or <code>delete</code> commands to add new parameters, labels, and values or to delete existing ones in any section of the Mobile IP configuration file.	“How to Add or Delete Configuration File Parameters” on page 610

Display the current settings of parameter destinations.	Uses the <code>mipagentconfig get</code> command to display current settings of any section of the Mobile IP configuration file.	“How to Display Current Parameter Values in the Configuration File” on page 611
---	--	---

Modifying the Mobile IP Configuration File

This section shows you how to modify the Mobile IP configuration file by using the `mipagentconfig` command. This section also shows you how to display the current settings of parameter destinations.

[“Configuring the Mobility IP Agent” on page 630](#) provides a conceptual description of the `mipagentconfig` command’s usage. You can also review the `mipagentconfig(1M)` man page.

▼ How to Modify the General Section

- Steps**
1. **Assume the Primary Administrator role, or become superuser on the system where you want to enable Mobile IP.**
The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.
 2. **On a command line, type the following command for each label that you want to modify in the General section.**

```
# mipagentconfig change <label> <value>
```

Example 27–1 Modifying a Parameter in the General Section

The following example shows how you might change the version number in the configuration file’s General section.

```
# mipagentconfig change version 2
```

▼ How to Modify the Advertisements Section

- Steps**
1. **Assume the Primary Administrator role, or become superuser, on the system where you want to enable Mobile IP.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Type the following command for each label that you want to modify in the `Advertisements` section:**

```
# mipagentconfig change adv device-name <label> <value>
```

For example, if you are changing the agent’s advertised lifetime to 300 seconds for device `hme0`, use the following command.

```
# mipagentconfig change adv hme0 AdvLifetime 300
```

Example 27–2 Modifying the `Advertisements` Section

The following example shows how you might change other parameters in the configuration file’s `Advertisements` section.

```
# mipagentconfig change adv hme0 HomeAgent yes
# mipagentconfig change adv hme0 ForeignAgent no
# mipagentconfig change adv hme0 PrefixFlags no
# mipagentconfig change adv hme0 RegLifetime 300
# mipagentconfig change adv hme0 AdvFrequency 4
# mipagentconfig change adv hme0 ReverseTunnel yes
```

▼ How to Modify the `GlobalSecurityParameters` Section

- Steps**
1. **Assume the Primary Administrator role, or become superuser, on the system where you want to enable Mobile IP.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Type the following command for each label that you want to modify in the `GlobalSecurityParameters` section:**

```
# mipagentconfig change <label> <value>
```

For example, if you are enabling home agent and foreign agent authentication, use the following command:

```
# mipagentconfig change HA-FAauth yes
```

Example 27–3 Modifying the `Global Security Parameters` Section

The following example shows how you might change other parameters in the configuration file’s `GlobalSecurityParameters` section.

```
# mipagentconfig change MaxClockSkew 200
# mipagentconfig change MN-FAauth yes
# mipagentconfig change Challenge yes
# mipagentconfig change KeyDistribution files
```

▼ How to Modify the Pool Section

- Steps** 1. **Assume the Primary Administrator role, or become superuser, on the system where you want to enable Mobile IP.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Type the following command for each label that you want to modify in the Pool section:**

```
# mipagentconfig change Pool pool-identifier <label> <value>
```

Example 27–4 Modifying the Pool Section

The following example shows the commands to use for changing the base address to 192.168.1.1 and the size of Pool 10 to 100.

```
# mipagentconfig change Pool 10 BaseAddress 192.168.1.1
# mipagentconfig change Pool 10 Size 100
```

▼ How to Modify the SPI Section

- Steps** 1. **Assume the Primary Administrator role, or become superuser, on the system where you want to enable Mobile IP.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Type the following command for each label that you want to modify in the SPI section:**

```
# mipagentconfig change SPI SPI-identifier <label> <value>
```

For example, if you are changing the key for SPI 257 to 5af2aee39ff0b332, use the following command.

```
# mipagentconfig change SPI 257 Key 5af2aee39ff0b332
```


Example 27-5 Modifying the SPI Section

The following example shows how to change the `ReplayMethod` label in the configuration file's SPI section.

```
# mipagentconfig change SPI 257 ReplayMethod timestamps
```

▼ How to Modify the Address Section

- Steps**
1. **Assume the Primary Administrator role, or become superuser, on the system where you want to enable Mobile IP.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Type the following command for each label that you want to modify in the Address section:**

```
# mipagentconfig change addr [NAI | IPaddr | node-default] <label> <value>
```

See “Address Section” on page 626 for a description of the three configuration methods (NAI, IP address, and node-default).

For example, if you are changing the SPI of IP address 10.1.1.1 to 258, use the following command:

```
# mipagentconfig change addr 10.1.1.1 SPI 258
```

Example 27-6 Modifying the Address Section

The following example shows how you can change other parameters that are provided in the sample configuration file's Address section.

```
# mipagentconfig change addr 10.1.1.1 Type agent
# mipagentconfig change addr 10.1.1.1 SPI 259
# mipagentconfig change addr mobilenode@abc.com Type node
# mipagentconfig change addr mobilenode@abc.com SPI 258
# mipagentconfig change addr mobilenode@abc.com Pool 2
# mipagentconfig change addr node-default SPI 259
# mipagentconfig change addr node-default Pool 3
# mipagentconfig change addr 10.68.30.36 Type agent
# mipagentconfig change addr 10.68.30.36 SPI 260
# mipagentconfig change IPsecRequest apply {auth_algs md5 sa shared}
```

▼ How to Add or Delete Configuration File Parameters

- Steps** 1. **Assume the Primary Administrator role, or become superuser, on the system where you want to enable Mobile IP.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Type the appropriate command for each label that you want to add or delete for the designated section:**

- For the General section use the following:

```
# mipagentconfig [add | delete] <label> <value>
```

- For the Advertisements section use the following:

```
# mipagentconfig [add | delete] adv device-name <label> <value>
```

Note – You can add an interface by typing the following:

```
# mipagentconfig add adv device-name
```

In this instance, default values are assigned to the interface (for both the foreign agent and the home agent).

- For the GlobalSecurityParameters, section use the following:

```
# mipagentconfig [add | delete] <label> <value>
```

- For the Pool section, use the following:

```
# mipagentconfig [add | delete] Pool pool-identifier <label> <value>
```

- For the SPI section, use the following:

```
# mipagentconfig [add | delete] SPI SPI-identifier <label> <value>
```

- For the Address section, use the following:

```
# mipagentconfig [add | delete] addr [NAI | IP-address | node-default] \  
<label> <value>
```

Note – Do not create identical Advertisements, Pool, SPI, and Address sections.

Example 27-7 Modifying File Parameters

For example, to create a new address pool, Pool 11, that has a base address of 192.167.1.1 and a size of 100, use the following commands.

```
# mipagentconfig add Pool 11 BaseAddress 192.167.1.1
# mipagentconfig add Pool 11 size 100
```

Example 27-8 Deleting SPI

The following example shows how to delete the SPI security parameter SPI 257.

```
# mipagentconfig delete SPI 257
```

▼ How to Display Current Parameter Values in the Configuration File

You can use the `mipagentconfig get` command to display current settings that are associated with parameter destinations.

Steps 1. Assume the Primary Administrator role, or become superuser, on the system where you are enabling Mobile IP.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Type the following command for each parameter for which you want to display settings:

```
# mipagentconfig get [<parameter> | <label>]
```

For example, if you are displaying the advertisement settings for the `hme0` device, use the following command:

```
# mipagentconfig get adv hme0
```

As a result, the following output might be displayed:

```
[Advertisements hme0]
  HomeAgent = yes
  ForeignAgent = yes
```

Example 27-9 Using the `mipagentconfig get` Command to Display Parameter Values

The following example shows the results of using the `mipagentconfig get` command with other parameter destinations.

```
# mipagentconfig get MaxClockSkew
  [GlobalSecurityParameters]
```


▼ How to Display Mobility Agent Status

- Steps** 1. **Become superuser or assume an equivalent role on the system where you are enabling Mobile IP.**

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Display the mobility agent status.**

```
# mipagentstat options

-f    Shows the list of active mobile nodes in the foreign agent’s visitor list.
-h    Shows the list of active mobile nodes in the home agent’s binding table.
-p    Shows the list of security associations with an agent’s mobility agent peers.
```

Example 27-10 Displaying Mobility Agent Status

This example shows how to display the visitor list for all mobile nodes that are registered with a foreign agent.

```
# mipagentstat -f
```

As a result, output similar to the following is displayed:

Mobile Node	Home Agent	Time (s) Granted	Time (s) Remaining	Flags
foobar.xyz.com	hal.xyz.com	600	125T.
10.1.5.23	10.1.5.1	1000	10T.

This example shows how to display foreign agent security associations.

```
# mipagentstat -p
```

As a result, output similar to the following is displayed:

Foreign Agent Security Association(s)			
	Requests	Replies	FTunnel	RTunnel
forn-agent.eng.sun.com	AH	AH	ESP	ESP

This example shows how to display home agent security associations.

```
# mipagentstat -fp
```

As a result, output similar to the following is displayed:

Home Agent Security Association(s)			
	Requests	Replies	FTunnel	RTunnel

home-agent.eng.sun.com	AH	AH	ESP	ESP
hal.xyz.com	AH,ESP	AH	AH,ESP	AH,ESP

Displaying Mobility Routes on a Foreign Agent

You can use the `netstat` command to display additional information about source-specific routes that are created by forward tunnels and reverse tunnels. See the `netstat(1M)` man page for more information about this command.

▼ How to Display Mobility Routes on a Foreign Agent

- Steps** 1. **Become superuser or assume an equivalent role on the system where you are enabling Mobile IP.**

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Display the mobility routes.**

```
# netstat -rn
```

Example 27-11 Displaying Mobility Routes on a Foreign Agent

The following example shows the routes for a foreign agent that uses a reverse tunnel.

```
Routing Table: IPv4 Source-Specific
Destination  In If      Source      Gateway  Flags  Use  Out If
-----
10.6.32.11   ip.tun1   --          10.6.32.97 UH       0    hme1
--          hme1     10.6.32.11 --        U        0    ip.tun1
```

The first line indicates that the destination IP address `10.6.32.11` and the incoming interface `ip.tun1` select `hme1` as the interface that forwards the packets. The next line indicates that any packet originating from interface `hme1` and source address `10.6.32.11` must be forwarded to `ip.tun1`.

Mobile IP Files and Commands (Reference)

This chapter describes the components that are provided with the Solaris implementation of Mobile IP. To use Mobile IP, you must first configure the Mobile IP configuration file by using the parameters and commands that are described in this chapter.

This chapter contains the following information:

- “Overview of the Solaris Mobile IP Implementation” on page 615
- “Mobile IP Configuration File” on page 616
- “Configuring the Mobility IP Agent” on page 630
- “Mobile IP Mobility Agent Status” on page 631
- “Mobile IP State Information” on page 632
- “netstat Extensions for Mobile IP” on page 632
- “snoop Extensions for Mobile IP” on page 633

Overview of the Solaris Mobile IP Implementation

The mobility agent software incorporates home agent and foreign agent functionality. The Solaris Mobile IP software does not provide a client mobile node. Only the agent functionality is provided. Each network with mobility support should have at least one static (non-mobile) host running this software.

The following RFC functions are supported in the Solaris implementation of Mobile IP:

- RFC 1918, “Address Allocation for Private Internets”
(<http://www.ietf.org/rfc/rfc1918.txt?number=1918>)
- RFC 2002, “IP Mobility Support” (Agent only)
(<http://www.ietf.org/rfc/rfc2002.txt?number=2002>)

- RFC 2003, "IP Encapsulation Within IP"
(<http://www.ietf.org/rfc/rfc2003.txt?number=2003>)
- RFC 2794, "Mobile IP Network Access Identifier Extension for IPv4"
(<http://www.ietf.org/rfc/rfc2794.txt?number=2794>)
- RFC 3012, "Mobile IPv4 Challenge/Response Extensions"
(<http://www.ietf.org/rfc/rfc3012.txt?number=3012>)
- RFC 3024, "Reverse Tunneling for Mobile IP"
(<http://www.ietf.org/rfc/rfc3024.txt?number=3024>)

The base Mobile IP protocol (RFC 2002) does not address the problem of scalable key distribution and treats key distribution as an orthogonal issue. The Solaris Mobile IP software utilizes only manually configured keys, specified in a configuration file.

The following RFC functions are not supported in the Solaris implementation of Mobile IP:

- RFC 1701, "General Routing Encapsulation"
(<http://www.ietf.org/rfc/rfc1701.txt?number=1701>)
- RFC 2004, "Minimal Encapsulation Within IP"
(<http://www.ietf.org/rfc/rfc2004.txt?number=2004>)

The following functions are not supported in the Solaris implementation of Mobile IP:

- The forwarding of multicast traffic or broadcast traffic by the home agent to the foreign agent for a mobile node that is visiting a foreign network
- The routing of broadcast and multicast datagrams through reverse tunnels
- Private care-of addresses or private home agent addresses

See the `mipagent(1M)` man page for additional information.

Mobile IP Configuration File

The `mipagent` command reads configuration information from the `/etc/inet/mipagent.conf` configuration file at startup. Mobile IP uses the `/etc/inet/mipagent.conf` configuration file to initialize the Mobile IP mobility agent. When configured and deployed, the mobility agent issues periodic router advertisements and responds to router discovery solicitation messages as well as Mobile IP registration messages.

See the `mipagent.conf(4)` man page for a description of file attributes. See the `mipagent(1M)` man page for a description of this file's usage.

Configuration File Format

The Mobile IP configuration file consists of sections. Each section has a unique name and is enclosed in square brackets. Each section contains one or more labels. You assign values to the labels by using the following format:

```
[Section_name]
    Label-name = value-assigned
```

“[Configuration File Sections and Labels](#)” on page 621 describes the section names, labels, and possible values.

Sample Configuration Files

The default Solaris installation provides the following sample configuration files in the `/etc/inet` directory:

- `mipagent.conf-sample` – Contains a sample configuration for a Mobile IP agent that provides both foreign agent and home agent functionality
- `mipagent.conf.fa-sample` – Contains a sample configuration for a Mobile IP agent that provides only foreign agent functionality
- `mipagent.conf.ha-sample` – Contains a sample configuration for a Mobile IP agent that provides only home agent functionality

These sample configuration files contain mobile node address and security settings. Before you can implement Mobile IP, you must create a configuration file with the name `mipagent.conf` and place it in the `/etc/inet` directory. This file contains the configuration settings that satisfy your Mobile IP implementation requirements. You can also choose one of the sample configuration files, modify it with your addresses and security settings, and copy it to `/etc/inet/mipagent.conf`.

For more information, see “[How to Create the Mobile IP Configuration File](#)” on page 601.

`mipagent.conf-sample` File

The following listing shows the sections, labels, and values that are contained in the `mipagent.conf-sample` file. “[Configuration File Sections and Labels](#)” on page 621 describes the syntax, sections, labels, and values.

```
[General]
    Version = 1.0    # version number for the configuration file. (required)

[Advertisements hme0]
    HomeAgent = yes
    ForeignAgent = yes
    PrefixFlags = yes
```


Configuration File Sections and Labels

The Mobile IP configuration file contains the following sections:

- General (Required)
- Advertisements (Required)
- GlobalSecurityParameters (Optional)
- Pool (Optional)
- SPI (Optional)
- Address (Optional)

The General and GlobalSecurityParameters sections contain information relevant to the operation of the Mobile IP agent. These sections can appear only once in the configuration file.

General Section

The General section contains only one label: the version number of the configuration file. The General section has the following syntax:

```
[General]
  Version = 1.0
```

Advertisements Section

The Advertisements section contains the HomeAgent and ForeignAgent labels, as well as other labels. You must include a different Advertisements section for each interface on the local host that provides Mobile IP services. The Advertisements section has the following syntax:

```
[Advertisements interface]
  HomeAgent = <yes/no>
  ForeignAgent = <yes/no>
  .
  .
```

Typically, your system has a single interface, such as eri0 or hme0, and supports both home agent and foreign agent operations. If this situation exists for the example hme0, then the yes value is assigned to both the HomeAgent and ForeignAgent labels as follows:

```
[Advertisements hme0]
  HomeAgent = yes
  ForeignAgent = yes
  .
  .
```

For advertisement over dynamic interfaces, use '*' for the device ID part. For example, *Interface-name* ppp* actually implies all PPP interfaces that are configured after the mipagent daemon has been started. All the attributes in the advertisement section of a dynamic interface type remain the same.

The following table describes the labels and values that you can use in the `Advertisements` section.

TABLE 28-1 Advertisements Section Labels and Values

Label	Value	Description
<code>HomeAgent</code>	yes or no	Determines if the <code>mipagent</code> daemon provides home agent functionality.
<code>ForeignAgent</code>	yes or no	Determines if <code>mipagent</code> provides foreign agent functionality.
<code>PrefixFlags</code>	yes or no	Specifies if advertisements include the optional prefix-length extension.
<code>AdvertiseOnBcast</code>	yes or no	If yes, advertisements are sent on <code>255.255.255.255</code> , rather than <code>224.0.0.1</code> .
<code>RegLifetime</code>	n	The maximum lifetime value that is accepted in registration requests, in seconds.
<code>AdvLifetime</code>	n	The maximum length of time that the advertisement is considered valid in the absence of further advertisements, in seconds.
<code>AdvFrequency</code>	n	Time between two consecutive advertisements, in seconds.
<code>ReverseTunnel</code>	yes or no FA or HA or both	Determines if <code>mipagent</code> provides reverse-tunnel functionality. The value <code>yes</code> means that both the foreign agent and home agent support reverse tunneling. The value <code>no</code> means that the interface does not support reverse tunneling. The value <code>FA</code> means that the foreign agent supports reverse tunneling. The value <code>HA</code> means that the home agent supports reverse tunneling. The value <code>both</code> means that both the foreign agent and home agent support reverse tunneling.

TABLE 28-1 Advertisements Section Labels and Values (Continued)

Label	Value	Description
ReverseTunnelRequired	yes or no	Determines if mipagent requires reverse tunnel functionality. Consequently, determines if a mobile node must request a reverse tunnel during registration. The value <i>yes</i> means that both the foreign agent and home agent require a reverse tunnel. The value <i>no</i> means that the interface does not require a reverse tunnel. The value <i>FA</i> means that the foreign agent requires a reverse tunnel. The value <i>HA</i> means that the home agent requires a reverse tunnel.
AdvInitCount	n	Determines the initial number of unsolicited advertisements. The default value is 1. This value is meaningful only if AdvLimitUnsolicited is <i>yes</i> .
AdvLimitUnsolicited	yes or no	Enables or disables a limited number of unsolicited advertisements over the mobility interface.

GlobalSecurityParameters Section

The GlobalSecurityParameters section contains the labels maxClockSkew, HA-FAauth, MN-FAauth, Challenge, and KeyDistribution. This section has the following syntax:

```
[GlobalSecurityParameters]
  MaxClockSkew = n
  HA-FAauth = <yes/no>
  MN-FAauth = <yes/no>
  Challenge = <yes/no>
  KeyDistribution = files
```

The Mobile IP protocol provides message replay protection by allowing timestamps to be present in the messages. If the clocks differ, the home agent returns an error to the mobile node with the current time and the mobile node can register again by using the current time. You use the MaxClockSkew label to configure the maximum number of seconds that differ between the home agent and the mobile node's clocks. The default value is 300 seconds.

The HA-FAauth and MN-FAauth labels enable or disable the requirement for home-foreign and mobile-foreign authentication, respectively. The default value is disabled. You use the challenge label so that the foreign agent issues challenges to the mobile node in its advertisements. The label is used for replay protection. The default value is disabled here, also.

The following table describes the labels and values that you can use in the `GlobalSecurityParameters` section.

TABLE 28-2 GlobalSecurityParameters Section Labels and Values

Label	Value	Description
MaxClockSkew	n	The number of seconds that <code>mipagent</code> accepts as a difference between its own local time and the time that is found in registration requests
HA-FAauth	yes or no	Specifies if HA-FA authentication extensions must be present in registration requests and replies
MN-FAauth	yes or no	Specifies if MN-FA authentication extensions must be present in registration requests and replies
Challenge	yes or no	Specifies if the foreign agent includes challenges in its mobility advertisements
KeyDistribution	files	Must be set to files

Pool Section

Mobile nodes can be assigned dynamic addresses by the home agent. Dynamic address assignment is done within the `mipagent` daemon independently of DHCP. You can create an address pool that can be used by mobile nodes by requesting a home address. Address pools are configured through the `Pool` section in the configuration file.

The `Pool` section contains the `BaseAddress` and `Size` labels. The `Pool` section has the following syntax:

```
[Pool pool-identifier]  
  BaseAddress = IP-address  
  Size = size
```

Note – If you use a `Pool` identifier, then it must also exist in the mobile node's `Address` section.

You use the `Pool` section to define address pools that can be assigned to the mobile nodes. You use the `BaseAddress` label to set the first IP address in the pool. You use the `Size` label to specify the number of addresses available in the pool.

For example, if IP addresses `192.168.1.1` through `192.168.1.100` are reserved in pool 10, the `Pool` section has the following entry:

```
[Pool 10]  
  BaseAddress = 192.168.1.1  
  Size = 100
```

Note – Address ranges should not encompass the broadcast address. For example, you should not assign `BaseAddress = 192.168.1.200` and `Size = 60`, because this range encompasses the broadcast address `192.168.1.255`.

The following table describes the labels and values that are used in the `Pool` section.

TABLE 28-3 `Pool` Section Labels and Values

Label	Value	Description
<code>BaseAddress</code>	<code>n.n.n.n</code>	First address in the address pool
<code>Size</code>	<code>n</code>	Number of addresses in the pool

SPI Section

Because the Mobile IP protocol requires message authentication, you must identify the security context by using a security parameter index (SPI). You define the security context in the `SPI` section. You must include a different `SPI` section for each security context that is defined. A numerical ID identifies the security context. The Mobile IP protocol reserves the first 256 SPIs. Therefore, you should use only SPI values greater than 256. The `SPI` section contains security-related information, such as shared secrets and replay protection.

The `SPI` section also contains the `ReplayMethod` and `Key` labels. The `SPI` section has the following syntax:

```
[SPI SPI-identifier]
  ReplayMethod = <none/timestamps>
  Key = key
```

Two communicating peers must share the same SPI identifier. You must configure them with the same key and replay method. You specify the key as a string of hexadecimal digits. The maximum length is 16 bytes. For example, if the key is 16 bytes long, and contains the hexadecimal values 0 through f, the key string might resemble the following:

```
Key = 0102030405060708090a0b0c0d0e0f10
```

Keys must have an even number of digits, corresponding to the two digits per byte representation.

The following table describes the labels and values that you can use in the `SPI` section.

TABLE 28-4 SPI Section Labels and Values

Label	Value	Description
ReplayMethod	none or timestamps	Specifies the type of replay authentication used for the SPI
Key	x	Authentication key in hexadecimal

Address Section

The Solaris implementation of Mobile IP enables you to configure mobile nodes using one of three methods. Each method is configured in the `Address` section. The first method follows the traditional Mobile IP protocol, and requires that each mobile node have a home address. The second method enables a mobile node to be identified through its Network Access Identifier (NAI). The last method enables you to configure a *default* mobile node, which can be used by any mobile node that has the proper SPI value and related keying material.

Mobile Node

The `Address` section for a mobile node contains the `Type` and `SPI` labels that define the address type and SPI identifier. The `Address` section has the following syntax:

```
[Address address]
  Type = node
  SPI = SPI-identifier
```

You must include an `Address` section in a home agent's configuration file for each mobile node that is supported.

If Mobile IP message authentication is required between the foreign agent and home agent, you must include an `Address` section for each peer with which an agent needs to communicate.

The SPI value that you configure must represent an SPI section that is present in the configuration file.

You can also configure private addresses for a mobile node.

The following table describes the labels and values that you can use in the `Address` section for a mobile node.

TABLE 28-5 Address Section Labels and Values (Mobile Node)

Label	Value	Description
Type	node	Specifies that the entry is for a mobile node

TABLE 28-5 Address Section Labels and Values (Mobile Node) (Continued)

Label	Value	Description
SPI	n	Specifies the SPI value for the associated entry

Mobility Agent

The Address section for a mobility agent contains the Type and SPI labels that define the address type and SPI identifier. This section also contains IPsec request, reply, and tunnel labels. The Address section for a mobility agent has the following syntax:

```
[Address address]
  Type = agent
  SPI = SPI-identifier
  IPsecRequest = action {properties} [: action {properties}]
  IPsecReply = action {properties} [: action {properties}]
  IPsecTunnel = action {properties} [: action {properties}]
```

You must include an Address section in a home agent's configuration file for each mobility agent that is supported.

If Mobile IP message authentication is required between the foreign agent and the home agent, you must include an Address section for each peer with which an agent needs to communicate.

The SPI value that you configure must represent an SPI section that is present in the configuration file.

The following table describes the labels and values that you can use in the Address section for a mobility agent.

TABLE 28-6 Address Section Labels and Values (Mobility Agent)

Label	Value	Description
Type	agent	Specifies that the entry is for a mobility agent
SPI	n	Specifies the SPI value for the associated entry
IPsecRequest	apply or permit (see following note)	IPsec properties to invoke for registration requests to and from this mobility agent peer
IPsecReply	apply or permit (see following note)	IPsec properties to invoke for registration replies to and from this mobility agent peer

TABLE 28-6 Address Section Labels and Values (Mobility Agent) (Continued)

Label	Value	Description
IPsecTunnel	apply or permit (see following note)	IPsec properties to invoke for tunnel traffic to and from this mobility agent peer

Note – The apply values correspond to outbound datagrams. The permit values correspond to inbound datagrams. Therefore, IPsecRequest apply values and IPsecReply permit values are used by the foreign agent to send and receive registration datagrams. The IPsecRequest permit values and the IPsecReply apply values are used by the home agent to receive and send registration datagrams.

Mobile Node Identified by Its NAI

The Address section for a mobile node that is identified by its NAI contains the Type, SPI, and Pool labels. The NAI parameter enables you to identify mobile nodes through their NAI. The Address section, using the NAI parameter, has the following syntax:

```
[Address NAI]
  Type = Node
  SPI = SPI-identifier
  Pool = pool-identifier
```

To use pools, you identify mobile nodes through their NAI. The Address section permits you to configure an NAI, as opposed to a home address. An NAI uses the format user@domain. You use the Pool label to specify which address pool to use in order to allocate the home address to the mobile node.

The following table describes the labels and values that you can use in the Address section for a mobile node that is identified by its NAI.

TABLE 28-7 Address Section Labels and Values (Mobile Node Identified by Its NAI)

Label	Value	Description
Type	node	Specifies that the entry is for a mobile node
SPI	n	Specifies the SPI value for the associated entry
Pool	n	Allocates the pool from which an address is assigned to a mobile node

You must have corresponding SPI and Pool sections for the SPI and Pool labels that are defined in an Address section with a mobile node that is identified by its NAI, as shown in the following figure.

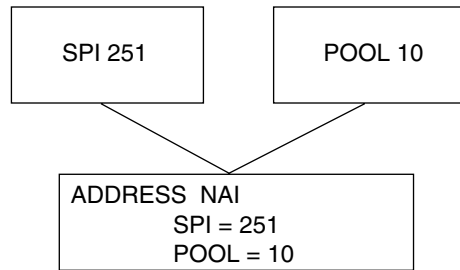


FIGURE 28-1 Corresponding SPI and Pool Sections for Address Section With Mobile Node Identified by Its NAI

Default Mobile Node

The Address section for a default mobile node contains the `Type`, `SPI`, and `Pool` labels. The `Node-Default` parameter enables you to permit all mobile nodes to get service if they have the correct SPI (defined in this section). The Address section, using the `Node-Default` parameter, has the following syntax:

```
[Address Node-Default]
  Type = Node
  SPI = SPI-identifier
  Pool = pool-identifier
```

The `Node-Default` parameter enables you to reduce the size of the configuration file. Otherwise, each mobile node requires its own section. However, the `Node-Default` parameter does pose a security risk. If a mobile node is no longer trusted for any reason, you need to update the security information on all trusted mobile nodes. This task can be very tedious. However, you can use the `Node-Default` parameter in networks that consider security risks unimportant.

The following table describes the labels and values that you can use in the Address section for a default mobile node.

TABLE 28-8 Address Section Labels and Values (Default Mobile Node)

Label	Value	Description
Type	node	Specifies that the entry is for a mobile node
SPI	n	Specifies the SPI value for the associated entry
Pool	n	Allocates the pool from which an address is assigned to a mobile node

You must have corresponding `SPI` and `Pool` sections for the `SPI` and `Pool` labels that are defined in the Address section with a default mobile node, as shown in the following figure.

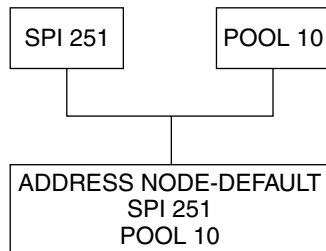


FIGURE 28-2 Corresponding SPI and Pool Sections for Address Section With a Default Mobile Node

Configuring the Mobility IP Agent

You can use the `mipagentconfig` command to configure the mobility agent. This command enables you to create or modify any parameter in the `/etc/inet/mipagent.conf` configuration file. Specifically, you can change any setting. Also, you can add or delete mobility clients, pools, and SPIs. The `mipagentconfig` command has the following syntax:

```
# mipagentconfig <command> <parameter> <value>
```

The following table describes the commands that you can use with `mipagentconfig` to create or modify parameters in the `/etc/inet/mipagent.conf` configuration file.

TABLE 28-9 `mipagentconfig` Subcommands

Command	Description
add	Used to add advertisement parameters, security parameters, SPIs, and addresses to the configuration file
change	Used to change advertisement parameters, security parameters, SPIs, and addresses in the configuration file
delete	Used to delete advertisement parameters, security parameters, SPIs, and addresses from the configuration file
get	Used to display current values in the configuration file

See the `mipagentconfig(1M)` man page for a description of command parameters and acceptable values. [“Modifying the Mobile IP Configuration File”](#) on page 606 provides procedures that use the `mipagentconfig` command.

Mobile IP Mobility Agent Status

You can use the `mipagentstat` command to display a foreign agent's visitor list and a home agent's binding table. You can also display the security associations with an agent's mobility agent peers. To display the foreign agent visitor list, you use the `mipagentstat` command's `-f` option. To display the home agent binding table, you use the `mipagentstat` command's `-h` option. To display the security associations with an agent's mobility agent peers, you use the `mipagentstat` command's `-p` option. The following examples show typical output when the `mipagentstat` command is used with these options.

EXAMPLE 28-1 Foreign Agent Visitor List

Mobile Node	Home Agent	Time (s) Granted	Time (s) Remaining	Flags
foobar.xyz.com	ha1.xyz.com	600	125T.
10.1.5.23	10.1.5.1	1000	10T.

EXAMPLE 28-2 Home Agent Binding Table

Mobile Node	Home Agent	Time (s) Granted	Time (s) Remaining	Flags
foobar.xyz.com	fa1.tuv.com	600	125T.
10.1.5.23	123.2.5.12	1000	10T.

EXAMPLE 28-3 Mobility Agent Peer Security Association Table

Foreign Agent Security Association(s)			
	Requests	Replies	FTunnel	RTunnel
forn-agent.eng.sun.com	AH	AH	ESP	ESP
Home Agent Security Association(s)			
	Requests	Replies	FTunnel	RTunnel
home-agent.eng.sun.com	AH	AH	ESP	ESP
ha1.xyz.com	AH,ESP	AH	AH,ESP	AH,ESP

See the `mipagentstat(1M)` man page for more information about the command's options. [“Displaying Mobility Agent Status” on page 612](#) provides procedures that use the `mipagentstat` command.

Mobile IP State Information

On shutdown, the `mipagent` daemon stores internal state information in `/var/inet/mipagent_state`. This event occurs only when the `mipagent` provides services as a home agent. This state information includes the list of mobile nodes that are being supported as a home agent, their current care-of addresses, and remaining registration lifetimes. This state information also includes the security association configuration with mobility agent peers. If the `mipagent` daemon is terminated for maintenance and restarted, `mipagent_state` is used to re-create as much of the mobility agent's internal state as possible. The intention is to minimize service disruption for mobile nodes that might be visiting other networks. If `mipagent_state` exists, it is read immediately after `mipagent.conf` every time `mipagent` is started or restarted.

netstat Extensions for Mobile IP

Mobile IP extensions have been added to the `netstat` command to identify Mobile IP forwarding routes. Specifically, you can use the `netstat` command to display a new routing table that is called "Source-Specific." See the `netstat(1M)` man page for more information.

The following example shows the output of `netstat` when you use the `-nr` flags.

EXAMPLE 28-4 Mobile IP Output From netstat Command

```
Routing Table: IPv4 Source-Specific
Destination   In If      Source      Gateway  Flags  Use  Out If
-----
10.6.32.11    ip.tun1    --          10.6.32.97 UH       0    hme1
--           hme1      10.6.32.11  --        U        0    ip.tun1
```

The example shows the routes for a foreign agent that uses a reverse tunnel. The first line indicates that the destination IP address `10.6.32.11` and the incoming interface `ip.tun1` select `hme1` as the interface that forwards the packets. The next line indicates that any packet that originates from interface `hme1` and source address `10.6.32.11` must be forwarded to `ip.tun1`.

snoop Extensions for Mobile IP

Mobile IP extensions have been added to the `snoop` command to identify Mobile IP traffic on the link. See the `snoop(1M)` man page for more information.

The following example shows the output of `snoop` that runs on the mobile node, `mip-mn2`.

EXAMPLE 28-5 Mobile IP Output From `snoop` Command

```
mip-mn2# snoop
Using device /dev/hme (promiscuous mode)
  mip-fa2 -> 224.0.0.1   ICMP Router advertisement (Lifetime 200s [1]:
{mip-fa2-80 2147483648}), (Mobility Agent Extension), (Prefix Lengths),
(padding)
  mip-mn2 -> mip-fa2   Mobile IP reg rqst
  mip-fa2 -> mip-mn2   Mobile IP reg reply (OK code 0)
```

This example shows that the mobile node received one of the periodically sent mobility agent advertisements from the foreign agent, `mip-fa2`. Then, `mip-mn2` sent a registration request to `mip-fa2`, and in response, received a registration reply. The registration reply indicates that the mobile node successfully registered with its home agent.

The `snoop` command also supports IPsec extensions. Consequently, you can show how registration and tunnel packets are being protected.

PART VI IPMP

This part introduces IP network multipathing (IPMP) and contains tasks for administering IPMP. IPMP provides failure detection and failover for interfaces on a system that are attached to the same link.

Introducing IPMP (Overview)

IP network multipathing (IPMP) provides physical interface failure detection and transparent network access failover for a system with multiple interfaces on the same IP link. IPMP also provides load spreading of packets for systems with multiple interfaces.

This chapter contains the following information:

- “Why You Should Use IPMP” on page 637
- “Basic Requirements of IPMP” on page 641
- “IPMP Addressing” on page 642
- “Solaris IPMP Components” on page 638
- “IPMP Interface Configurations” on page 644
- “IPMP Failure Detection and Recovery Features” on page 646
- “IPMP and Dynamic Reconfiguration” on page 649

For IPMP configuration tasks, refer to [Chapter 30](#).

Why You Should Use IPMP

IPMP provides increased reliability, availability, and network performance for systems with multiple physical interfaces. Occasionally, a physical interface or the networking hardware attached to that interface might fail or require maintenance. Traditionally, at that point, the system can no longer be contacted through any of the IP addresses that are associated with the failed interface. Additionally, any existing connections to the system using those IP addresses are disrupted.

By using IPMP, you can configure one or more physical interfaces into an IP multipathing group, or *IPMP group*. After configuring IPMP, the system automatically monitors the interfaces in the IPMP group for failure. If an interface in the group fails or is removed for maintenance, IPMP automatically migrates, or *fails over*, the failed

interface's IP addresses. The recipient of these addresses is a functioning interface in the failed interface's IPMP group. The failover feature of IPMP preserves connectivity and prevents disruption of any existing connections. Additionally, IPMP improves overall network performance by automatically spreading out network traffic across the set of interfaces in the IPMP group. This process is called *load spreading*.

Solaris IPMP Components

Solaris IPMP involves the following software:

- The `in.mpathd` daemon, which is explained fully in the `in.mpathd(1M)` man page.
- The `/etc/default/mpathd` configuration file, which is also described in the `in.mpathd(1M)` man page.
- `ifconfig` options for IPMP configuration, as described in the `ifconfig(1M)` man page.

Multipathing Daemon, `in.mpathd`

The `in.mpathd` daemon detects interface failures, and then implements various procedures for failover and failback. After `in.mpathd` detects a failure or a repair, the daemon sends an `ioctl` to perform the failover or failback. The `ip` kernel module, which implements the `ioctl`, does the network access failover transparently and automatically.

Note – Do not use Alternate Pathing while using IPMP on the same set of network interface cards. Likewise, you should not use IPMP while you are using Alternate Pathing. You can use Alternate Pathing and IPMP at the same time on different sets of interfaces. For more information about Alternate Pathing, refer to the *Sun Enterprise Server Alternate Pathing 2.3.1 User Guide*.

The `in.mpathd` daemon detects failures and repairs by sending out probes on all the interfaces that are part of an IPMP group. The `in.mpathd` daemon also detects failures and repairs by monitoring the `RUNNING` flag on each interface in the group. Refer to the `in.mpathd(1M)` man page for more information.

IPMP Terminology and Concepts

This section introduces terms and concepts that are used throughout [Part VI](#).

IP Link

In IPMP terminology, an *IP link* is a communication facility or medium over which nodes can communicate at the data-link layer of the Internet protocol suite. Types of IP links might include simple Ethernets, bridged Ethernets, hubs, or Asynchronous Transfer Mode (ATM) networks. An IP link can have one or more IPv4 subnet numbers, and, if applicable, one or more IPv6 subnet prefixes. A subnet number or prefix cannot be assigned to more than one IP link. In ATM LANE, an IP link is a single emulated local area network (LAN). With the Address Resolution Protocol (ARP), the scope of the ARP protocol is a single IP link.

Note – Other IP-related documents, such as RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, use the term *link* instead of *IP link*. Part VI uses the term *IP link* to avoid confusion with IEEE 802. In IEEE 802, *link* refers to a single wire from an Ethernet network interface card (NIC) to an Ethernet switch.

Physical Interface

The *physical interface* provides a system's attachment to an IP link. This attachment is often implemented as a device driver and a NIC. If a system has multiple interfaces attached to the same link, you can configure IPMP to perform failover if one of the interfaces fails. For more information on physical interfaces, refer to "[IPMP Interface Configurations](#)" on page 644.

Network Interface Card

A *network interface card* is a network adapter that can be built in to the system. Or, the NIC can be a separate card that serves as an interface from the system to an IP link. Some NICs can have multiple physical interfaces. For example, a `qfe` NIC can have four interfaces, `qfe0` through `qfe3`, and so on.

IPMP Group

An IP multipathing group, or *IPMP group*, consists of one or more physical interfaces on the same system that are configured with the same IPMP group name. All interfaces in the IPMP group must be connected to the same IP link. The same (non-null) character string IPMP group name identifies all interfaces in the group. You can place interfaces from NICs of different speeds within the same IPMP group, as long as the NICs are of the same type. For example, you can configure the interfaces of 100-megabit Ethernet NICs and the interfaces of one gigabit Ethernet NICs in the same group. As another example, suppose you have two 100-megabit Ethernet NICs. You can configure one of the interfaces down to 10 megabits and still place the two interfaces into the same IPMP group.

You cannot place two interfaces of different media types into an IPMP group. For example, you cannot place an ATM interface in the same group as an Ethernet interface.

Failure Detection and Failover

Failure detection is the process of detecting when an interface or the path from an interface to an Internet layer device no longer works. IPMP provides systems with the ability to detect when an interface has failed. IPMP detects the following types of communication failures:

- The transmit or receive path of the interface has failed.
- The attachment of the interface to the IP link is down.
- The port on the switch does not transmit or receive packets.
- The physical interface in an IPMP group is not present at system boot.

After detecting a failure, IPMP begins failover. *Failover* is the automatic process of switching the network access from a failed interface to a functioning physical interface in the same group. Network access includes IPv4 unicast, multicast, and broadcast traffic, as well as IPv6 unicast and multicast traffic. Failover can only occur when you have configured more than one interface in the IPMP group. The failover process ensures uninterrupted access to the network.

Repair Detection and Failback

Repair detection is the process of detecting when a NIC or the path from a NIC to an Internet layer device starts operating correctly after a failure. After detecting that a NIC has been repaired, IPMP performs *failback*, the process of switching network access back to the repaired interface. Repair detection assumes that you have enabled failbacks. See [“Detecting Physical Interface Repairs” on page 648](#) for more information.

Target Systems

Probe-based failure detection uses *target systems* to determine the condition of an interface. Each target system must be attached to the same IP link as the members of the IPMP group. The `in.mpathd` daemon on the local system sends ICMP probe messages to each target system. The probe messages help to determine the health of each interface in the IPMP group.

For more information about target system use in probe-based failure detection, refer to [“Probe-Based Failure Detection” on page 647](#).

Outbound Load Spreading

With IPMP configured, outbound network packets are spread across multiple NICs without affecting the ordering of packets. This process is known as *load spreading*. As a result of load spreading, higher throughput is achieved. Load spreading occurs only when the network traffic is flowing to multiple destinations that use multiple connections.

Dynamic Reconfiguration

Dynamic reconfiguration (DR) is the ability to reconfigure a system while the system is running, with little or no impact on existing operations. Not all Sun platforms support DR. Some Sun platforms might only support DR of certain types of hardware. On platforms that support DR of NIC's, IPMP can be used to transparently fail over network access, providing uninterrupted network access to the system.

For more information on how IPMP supports DR, refer to [“IPMP and Dynamic Reconfiguration” on page 649](#).

Basic Requirements of IPMP

IPMP is built into the Solaris Operating System (Solaris OS) and does not require any special hardware. Any interface that is supported by the Solaris OS can be used with IPMP. However, IPMP does impose the following requirements on your network configuration and topology:

- All interfaces in an IPMP group must have unique MAC addresses.
Note that by default, the network interfaces on SPARC based systems all share a single MAC address. Thus, you must explicitly change the default in order to use IPMP on SPARC based systems. For more information, refer to [“How to Plan for an IPMP Group” on page 655](#).
- All interfaces in an IPMP group must be of the same media type. For more information, refer to [“IPMP Group” on page 639](#).
- All interfaces in an IPMP group must be on the same IP link. For more information, refer to [“IPMP Group” on page 639](#).
- Depending on your failure detection requirements, you might need to either use specific types of network interfaces or configure additional IP addresses on each network interface. Refer to [“Link-Based Failure Detection” on page 646](#) and [“Probe-Based Failure Detection” on page 647](#).

IPMP Addressing

You can configure IPMP failure detection on both IPv4 networks and dual-stack, IPv4 and IPv6 networks. Interfaces that are configured with IPMP support two types of addresses: data addresses and test addresses.

Data Addresses

Data addresses are the conventional IPv4 and IPv6 addresses that are assigned to an interface of a NIC at boot time or manually, through the `ifconfig` command. The standard IPv4 and, if applicable, IPv6 packet traffic through an interface is considered to be *data traffic*.

Test Addresses

Test addresses are IPMP-specific addresses that are used by the `in.mpathd` daemon. For an interface to use probe-based failure and repair detection, that interface must be configured with at least one test address.

Note – You need to configure test addresses only if you want to use probe-based failure detection.

The `in.mpathd` daemon uses test addresses to exchange ICMP probes, also called *probe traffic*, with other targets on the IP link. Probe traffic helps to determine the status of the interface and its NIC, including whether an interface has failed. The probes verify that the send and receive path to the interface is working correctly.

Each interface can be configured with an IP test address. For an interface on a dual-stack network, you can configure an IPv4 test address, an IPv6 test address, or both IPv4 and IPv6 test addresses.

After an interface fails, the test addresses remain on the failed interface so that `in.mpathd` can continue to send probes to check for subsequent repair. You must specifically configure test addresses so that applications do not accidentally use them. For more information, refer to [“Preventing Applications From Using Test Addresses” on page 644](#).

For more information on probe-based failure detection, refer to [“Probe-Based Failure Detection” on page 647](#).

IPv4 Test Addresses

In general, you can use any IPv4 address on your subnet as a test address. IPv4 test addresses do not need to be routeable. Because IPv4 addresses are a limited resource for many sites, you might want to use non-routeable RFC 1918 private addresses as test addresses. Note that the `in.mpathd` daemon exchanges only ICMP probes with other hosts on the same subnet as the test address. If you do use RFC 1918-style test addresses, be sure to configure other systems, preferably routers, on the IP link with addresses on the appropriate RFC 1918 subnet. The `in.mpathd` daemon can then successfully exchange probes with target systems.

The IPMP examples use RFC 1918 addresses from the `192.168.0/24` network as IPv4 test addresses. For more information about RFC 1918 private addresses, refer to RFC 1918, Address Allocation for Private Internets. (<http://www.ietf.org/rfc/rfc1918.txt?number=1918>)

To configure IPv4 test addresses, refer to the task “[How to Configure an IPMP Group With Multiple Interfaces](#)” on page 659.

IPv6 Test Addresses

The only valid IPv6 test address is the link-local address of a physical interface. You do not need a separate IPv6 address to serve as an IPMP test address. The IPv6 link-local address is based on the Media Access Control (MAC) address of the interface. Link-local addresses are automatically configured when the interface becomes IPv6-enabled at boot time or when the interface is manually configured through `ifconfig`.

To identify the link-local address of an interface, run the `ifconfig interface` command on an IPv6-enabled node. Check the output for the address that begins with the prefix `fe80`, the link-local prefix. The `NOFAILOVER` flag in the following `ifconfig` output indicates that the link-local address `fe80::a00:20ff:feb9:17fa/10` of the `hme0` interface is used as the test address.

```
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:17fa/10
```

For more information on link-local addresses, refer to “[Link-Local Unicast Address](#)” on page 79.

When an IPMP group has both IPv4 and IPv6 plumbed on all the group’s interfaces, you do not need to configure separate IPv4 test addresses. The `in.mpathd` daemon can use the IPv6 link-local addresses as test addresses.

To create an IPv6 test address, refer to the task “[How to Configure an IPMP Group With Multiple Interfaces](#)” on page 659.

Preventing Applications From Using Test Addresses

After you have configured a test address, you need to ensure that this address is not used by applications. Otherwise, if the interface fails, the application is no longer reachable because test addresses do not fail over during the failover operation. To ensure that IP does not choose the test address for normal applications, mark the test address as `deprecated`.

IPv4 does not use a deprecated address as a source address for any communication, unless an application explicitly binds to the address. The `in.mpathd` daemon explicitly binds to such an address in order to send and receive probe traffic.

Because IPv6 link-local addresses are usually not present in a name service, DNS and NIS applications do not use link-local addresses for communication. Consequently, you must not mark IPv6 link-local addresses as `deprecated`.

IPv4 test addresses should not be placed in the DNS and NIS name service tables. In IPv6, link-local addresses are not normally placed in the name service tables.

IPMP Interface Configurations

An IPMP configuration typically consists of two or more physical interfaces on the same system that are attached to the same IP link. These physical interfaces might or might not be on the same NIC. The interfaces are configured as members of the same IPMP group. If the system has additional interfaces on a second IP link, you must configure these interfaces as another IPMP group.

A single interface can be configured in its own IPMP group. The single interface IPMP group has the same behavior as an IPMP group with multiple interfaces. However, failover and failback cannot occur for an IPMP group with only one interface.

Standby Interfaces in an IPMP Group

The *standby interface* in an IPMP group is not used for data traffic unless some other interface in the group fails. When a failure occurs, the data addresses on the failed interface migrate to the standby interface. Then, the standby interface is treated the same as other active interfaces until the failed interface is repaired. Some failovers might not choose a standby interface. Instead, these failovers might choose an active interface with fewer data addresses that are configured as UP than the standby interface.

You should configure only test addresses on a standby interface. IPMP does not permit you to add a data address to an interface that is configured through the `ifconfig` command as `standby`. Any attempt to create this type of configuration will fail. Similarly, if you configure as `standby` an interface that already has data addresses, these addresses automatically fail over to another interface in the IPMP group. Due to these restrictions, you must use the `ifconfig` command to mark any test addresses as `deprecated` and `-failover` prior to setting the interface as `standby`. To configure standby interfaces, refer to [“How to Configure a Standby Interface for an IPMP Group”](#) on page 665.

Common IPMP Interface Configurations

As mentioned in [“IPMP Addressing”](#) on page 642, interfaces in an IPMP group handle regular data traffic and probe traffic, depending on the interfaces’ configuration. You use IPMP options of the `ifconfig` command to create the configuration.

An *active interface* is a physical interface that transmits both data traffic and probe traffic. You configure the interface as “active” by performing either the task [“How to Configure an IPMP Group With Multiple Interfaces”](#) on page 659 or the task [“How to Configure a Single Interface IPMP Group”](#) on page 667.

The following are two common types of IPMP configurations:

- | | |
|-------------------------------------|---|
| Active-active configuration | A two interface IPMP group where both interfaces are “active,” that is they might be transmitting both probe and data traffic at all times. |
| Active-standby configuration | A two interface IPMP group where one interface is configured as “standby.” |

Checking the Status of an Interface

You can check the status of an interface by issuing the `ifconfig interface` command. For general information on `ifconfig` status reporting, refer to [“How to Get Information About a Specific Interface”](#) on page 153.

For example, you can use the `ifconfig` command to obtain the status of a standby interface. When the standby interface is not hosting any data address, the interface has the `INACTIVE` flag for its status. You can observe this flag in the status lines for the interface in the `ifconfig` output.

IPMP Failure Detection and Recovery Features

The `in.mpathd` daemon handles the following types of failure detection:

- Link-based failure detection, if supported by the NIC driver
- Probe-based failure detection, when test addresses are configured
- Detection of interfaces that were missing at boot time

The `in.mpathd(1M)` man page completely describes how the `in.mpathd` daemon handles the detection of interface failures.

Link-Based Failure Detection

Link-based failure detection is always enabled, provided that the interface supports this type of failure detection. The following Sun network drivers are supported in the current release of the Solaris OS:

- `hme`
- `eri`
- `ce`
- `ge`
- `bge`
- `qfe`
- `dmfe`

To determine whether a third-party interface supports link-based failure detection, refer to the manufacturer's documentation.

These network interface drivers monitor the interface's link state and notify the networking subsystem when that link state changes. When notified of a change, the networking subsystem either sets or clears the `RUNNING` flag for that interface, as appropriate. When the daemon detects that the interface's `RUNNING` flag has been cleared, the daemon immediately fails the interface.

Probe-Based Failure Detection

The `in.mpathd` daemon performs probe-based failure detection on each interface in the IPMP group that has a test address. Probe-based failure detection involves the sending and receiving of ICMP probe messages that use test addresses. These messages go out over the interface to one or more target systems on the same IP link. For an introduction to test addresses, refer to [“Test Addresses” on page 642](#). For information on configuring test addresses, refer to [“How to Configure an IPMP Group With Multiple Interfaces” on page 659](#).

The `in.mpathd` daemon determines which target systems to probe dynamically. Routers that are connected to the IP link are automatically selected as targets for probing. If no routers exist on the link, `in.mpathd` sends probes to neighbor hosts on the link. A multicast packet that is sent to the all hosts multicast address, `224.0.0.1` in IPv4 and `ff02::1` in IPv6, determines which hosts to use as target systems. The first few hosts that respond to the echo packets are chosen as targets for probing. If `in.mpathd` cannot find routers or hosts that responded to the ICMP echo packets, `in.mpathd` cannot detect probe-based failures.

You can use host routes to explicitly configure a list of target systems to be used by `in.mpathd`. For instructions, refer to [“Configuring Target Systems” on page 663](#).

To ensure that each interface in the IPMP group functions properly, `in.mpathd` probes all the targets separately through all the interfaces in the IPMP group. If no replies are made in response to five consecutive probes, `in.mpathd` considers the interface to have failed. The probing rate depends on the *failure detection time* (FDT). The default value for failure detection time is 10 seconds. However, you can tune the failure detection time in the `/etc/default/mpathd` file. For instructions, go to [“How to Configure the /etc/default/mpathd File” on page 677](#).

For a failure detection time of 10 seconds, the probing rate is approximately one probe every two seconds. The actual time that is needed to detect an interface failure can take from 20 seconds to a few minutes. The time depends on the system and network load. The failure detection time applies only to probe-based failure detection.

Group Failures

A *group failure* occurs when all interfaces in an IPMP group appear to fail at the same time. The `in.mpathd` daemon does not perform failovers for a group failure. Also, no failover occurs when all the target systems fail at the same time. In this instance, `in.mpathd` flushes all of its current target systems and discovers new target systems.

Detecting Physical Interface Repairs

For the `in.mpathd` daemon to consider an interface to be repaired, the `RUNNING` flag must be set for the interface. If probe-based failure detection is used, the `in.mpathd` daemon must receive responses to 10 consecutive probe packets from the interface before that interface is considered repaired. When an interface is considered repaired, any addresses that failed over to another interface then fail back to the repaired interface. If the interface was configured as “active” before it failed, after repair that interface can resume sending and receiving traffic.

What Happens During Interface Failover

The following two examples show a typical configuration and how that configuration automatically changes when an interface fails. When the `hme0` interface fails, notice that all data addresses move from `hme0` to `hme1`.

EXAMPLE 29–1 Interface Configuration Before an Interface Failure

```
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.85.19 netmask ffffffff broadcast 192.168.85.255
    groupname test
hme0:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1500
    index 2 inet 192.168.85.21 netmask ffffffff broadcast 192.168.85.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
8    inet 192.168.85.20 netmask ffffffff broadcast 192.168.85.255
    groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1500
    index 2 inet 192.168.85.22 netmask ffffffff broadcast 192.168.85.255
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
    inet6 fe80::a00:20ff:feb9:19fa/10
    groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
    inet6 fe80::a00:20ff:feb9:1bfc/10
    groupname test
```

EXAMPLE 29–2 Interface Configuration After an Interface Failure

```
hme0: flags=19000842<BROADCAST,RUNNING,MULTICAST,IPv4,NOFAILOVER,FAILED> mtu 0 index 2
    inet 0.0.0.0 netmask 0
    groupname test
hme0:1: flags=19040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER,FAILED>
    mtu 1500 index 2 inet 192.168.85.21 netmask ffffffff broadcast 10.0.0.255
hme1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.85.20 netmask ffffffff broadcast 192.168.85.255
    groupname test
hme1:1: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1500
    index 2 inet 192.168.85.22 netmask ffffffff broadcast 10.0.0.255
hme1:2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 6
    inet 192.168.85.19 netmask ffffffff broadcast 192.168.18.255
```


EXAMPLE 29-2 Interface Configuration After an Interface Failure (Continued)

```
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER,FAILED> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:19fa/10
      groupname test
hme1: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:1bfc/10
      groupname test
```

You can see that the `FAILED` flag is set on `hme0` to indicate that this interface has failed. You can also see that `hme1:2` has been created. `hme1:2` was originally `hme0`. The address `192.168.85.19` then becomes accessible through `hme1`.

Multicast memberships that are associated with `192.168.85.19` can still receive packets, but they now receive packets through `hme1`. When the failover of address `192.168.85.19` from `hme0` to `hme1` occurred, a dummy address `0.0.0.0` was created on `hme0`. The dummy address was created so that `hme0` can still be accessed. `hme0:1` cannot exist without `hme0`. The dummy address is removed when a subsequent failback takes place.

Similarly, failover of the IPv6 address from `hme0` to `hme1` occurred. In IPv6, multicast memberships are associated with interface indexes. Multicast memberships also fail over from `hme0` to `hme1`. All the addresses that `in.ndpd` configured also moved. This action is not shown in the examples.

The `in.mpathd` daemon continues to probe through the failed interface `hme0`. After the daemon receives 10 consecutive replies for a default repair detection time of 20 seconds, the daemon determines that the interface is repaired. Because the `RUNNING` flag is also set on `hme0`, the daemon invokes the failback. After failback, the original configuration is restored.

For a description of all error messages that are logged on the console during failures and repairs, see the `in.mpathd(1M)` man page.

IPMP and Dynamic Reconfiguration

The dynamic reconfiguration (DR) feature enables you to reconfigure system hardware, such as interfaces, while the system is running. This section explains how DR interoperates with IPMP.

On a system that supports DR of NICs, IPMP can be used to preserve connectivity and prevent disruption of existing connections. You can safely attach, detach, or reattach NIC's on a system that supports DR and uses IPMP. This is possible because IPMP is integrated into the Reconfiguration Coordination Manager (RCM) framework. RCM manages the dynamic reconfiguration of system components.

You typically use the `cfgadm` command to perform DR operations. However, some platforms provide other methods. Consult your platform's documentation for details. You can find specific documentation about DR from the following resources.

TABLE 29-1 Documentation Resources for Dynamic Reconfiguration

Description	For Information
Detailed information on the <code>cfgadm</code> command	<code>cfgadm(1M)</code> man page
Specific information about DR in the Sun Cluster environment	<i>Sun Cluster 3.1 System Administration Guide</i>
Specific information about DR in the Sun Fire environment	<i>Sun Fire 880 Dynamic Reconfiguration Guide</i>
Introductory information about DR and the <code>cfgadm</code> command	Chapter 6, "Dynamically Configuring Devices (Tasks)," in <i>System Administration Guide: Devices and File Systems</i>
Tasks for administering IPMP groups on a system that supports DR	"Replacing a Failed Physical Interface on Systems That Support Dynamic Reconfiguration" on page 672

Attaching NICs

You can add interfaces to an IPMP group at any time by using the `ifconfig` command, as explained in ["How to Configure an IPMP Group With Multiple Interfaces" on page 659](#). Thus, any interfaces on system components that you attach after system boot can be plumbed and added to an existing IPMP group. Or, if appropriate, you can configure the newly added interfaces into their own IPMP group.

These interfaces and the data addresses that are configured on them are immediately available for use by the IPMP group. However, for the system to automatically configure and use the interfaces after a reboot, you must create an `/etc/hostname.interface` file for each new interface. For instructions, refer to ["How to Add a Physical Interface After Installation" on page 113](#).

If an `/etc/hostname.interface` file already exists when the interface is attached, then RCM automatically configures the interface according to the contents of this file. Thus, the interface receives the same configuration that it would have received after system boot.

Detaching NICs

All requests to detach system components that contain NICs are first checked to ensure that connectivity can be preserved. For instance, by default you cannot detach a NIC that is not in an IPMP group. You also cannot detach a NIC that contains the only functioning interfaces in an IPMP group. However, if you must remove the system component, you can override this behavior by using the `-f` option of `cfgadm`, as explained in the `cfgadm(1M)` man page.

If the checks are successful, the data addresses associated with the detached NIC fail over to a functioning NIC in the same group, as if the NIC being detached had failed. When the NIC is detached, all test addresses on the NIC's interfaces are unconfigured. Then, the NIC is unplumbed from the system. If any of these steps fail, or if the DR of other hardware on the same system component fails, then the previous configuration is restored to its original state. You should receive a status message regarding this event. Otherwise, the detach request completes successfully. You can remove the component from the system. No existing connections are disrupted.

Reattaching NICs

RCM records the configuration information associated with any NIC's that are detached from a running system. As a result, RCM treats the reattachment of a NIC that had been previously detached identically as it would to the attachment of a new NIC. That is, RCM only performs plumbing.

However, reattached NICs typically have an existing `/etc/hostname.interface` file. In this case, RCM automatically configures the interface according to the contents of the existing `/etc/hostname.interface` file. Additionally, RCM informs the `in.mpathd` daemon of each data address that was originally hosted on the reattached interface. Thus, once the reattached interface is functioning properly, all of its data addresses are failed back to the reattached interface as if it had been repaired.

If the NIC being reattached does not have an `/etc/hostname.interface` file, then no configuration information is available. RCM has no information regarding how to configure the interface. One consequence of this situation is that addresses that were previously failed over to another interface are not failed back.

NICs That Were Missing at System Boot

NICs that are not present at system boot represent a special instance of failure detection. At boot time, the startup scripts track any interfaces with `/etc/hostname.interface` files that cannot be plumbed. Any data addresses in such an interface's `/etc/hostname.interface` file are automatically hosted on an alternative interface in the IPMP group.

In such an event, you receive error messages similar to the following

```
moving addresses from failed IPv4 interfaces: hme0 (moved to hme1)
moving addresses from failed IPv6 interfaces: hme0 (moved to hme1)
```

If no alternative interface exists, you receive error messages similar to the following:

```
moving addresses from failed IPv4 interfaces: hme0 (couldn't move; no alternative interface)
moving addresses from failed IPv6 interfaces: hme0 (couldn't move; no alternative interface)
```

Note – In this instance of failure detection, only data addresses that are explicitly specified in the missing interface's `/etc/hostname.interface` file move to an alternative interface. Any addresses that are usually acquired through other means, such as through RARP or DHCP, are not acquired or moved.

If an interface with the same name as another interface that was missing at system boot is reattached using DR, RCM automatically plumbs the interface. Then, RCM configures the interface according to the contents of the interface's `/etc/hostname.interface` file. Finally, RCM fails back any data addresses, just as if the interface had been repaired. Thus, the final network configuration is identical to the configuration that would have been made if the system had been booted with the interface present.

Administering IPMP (Tasks)

This chapter provides tasks for administering interface groups with IP network multipathing (IPMP). The following major topics are discussed:

- “Configuring IPMP (Task Maps)” on page 653
- “Configuring IPMP Groups” on page 655
- “Maintaining IPMP Groups” on page 668
- “Replacing a Failed Physical Interface on Systems That Support Dynamic Reconfiguration” on page 672
- “Recovering a Physical Interface That Was Not Present at System Boot” on page 674
- “Modifying the `/etc/default/mpathd` IPMP Configuration File” on page 677

For an overview of IPMP concepts, refer to [Chapter 29](#).

Configuring IPMP (Task Maps)

This section contains links to the tasks that are described in this chapter.

Configuring and Administering IPMP Groups (Task Map)

Task	Description	For Instructions
Plan for an IPMP group.	Lists all ancillary information and required tasks before you can configure an IPMP group.	“How to Plan for an IPMP Group” on page 655
Configure an IPMP interface group with multiple interfaces.	Configures multiple interfaces as members of an IPMP group.	“How to Configure an IPMP Group With Multiple Interfaces” on page 659
Configure an IPMP group where one of the interfaces is a standby interface.	Configures one of the interfaces in a multiple interface IPMP group as a standby interface.	“How to Configure a Standby Interface for an IPMP Group” on page 665
Configure an IPMP group that consists of a single interface.	Creates a single interface IPMP group.	“How to Configure a Single Interface IPMP Group” on page 667
Display the IPMP group to which a physical interface belongs.	Explains how to obtain the name of an interface’s IPMP group from the output of the <code>ifconfig</code> command.	“How to Display the IPMP Group Membership of an Interface” on page 669
Add an interface to an IPMP group.	Configures a new interface as a member of an existing IPMP group.	“How to Add an Interface to an IPMP Group” on page 669
Remove an interface from an IPMP group.	Explains how to remove an interface from an IPMP group.	“How to Remove an Interface From an IPMP Group” on page 670
Move an interface from an existing IPMP group to a different group.	Moves interfaces among IPMP groups.	“How to Move an Interface From One IPMP Group to Another Group” on page 671
Change three default settings for the <code>in.mpathd</code> daemon.	Customizes failure detection time and other parameters of the <code>in.mpathd</code> daemon.	“How to Configure the <code>/etc/default/mpathd</code> File” on page 677

Administering IPMP on Interfaces That Support Dynamic Reconfiguration (Task Map)

Task	Description	For Instructions
Remove an interface that has failed.	Removes a failed interface on a system.	“How to Remove a Physical Interface That Has Failed (DR-Detach)” on page 672
Replace an interface that has failed.	Replaces a failed interface.	“How to Replace a Physical Interface That Has Failed (DR-Attach)” on page 673
Recover an interface that was not configured at boot time.	Recovers a failed interface.	“How to Recover a Physical Interface That Was Not Present at System Boot” on page 675

Configuring IPMP Groups

This section provides procedures for configuring IPMP groups. It also describes how to configure an interface as a standby.

Planning for an IPMP Group

Before you configure interfaces on a system as part of an IPMP group, you need to do some preconfiguration planning.

▼ How to Plan for an IPMP Group

The following procedure includes the planning tasks and information to be gathered prior to configuring the IPMP group. The tasks do not have to be performed in sequence.

Steps 1. **Decide which interfaces on the system are to be part of the IPMP group.**

An IPMP group usually consists of at least two physical interfaces that are connected to the same IP link. However, you can configure a single interface IPMP group, if required. For an introduction to IPMP groups, refer to [“IPMP Interface Configurations” on page 644](#). For example, you can configure the same Ethernet

switch or the same IP subnet under the same IPMP group. You can configure any number of interfaces into the same IPMP group.

You cannot use the `group` parameter of the `ifconfig` command with logical interfaces. For example, you can use the `group` parameter with `hme0`, but not with `hme0:1`.

2. Verify that each interface in the group has a unique MAC address.

For instructions, refer to “SPARC: How to Ensure That the MAC Address of an Interface Is Unique” on page 657.

3. Choose a name for the IPMP group.

Any non-null name is appropriate for the group. You might want to use a name that identifies the IP link to which the interfaces are attached.

4. Ensure that the same set of STREAMS modules is pushed and configured on all interfaces in the IPMP group.

All interfaces in the same group must have the same STREAMS modules configured in the same order.

a. Check the order of STREAMS modules on all interfaces in the prospective IPMP group.

You can print out a list of STREAMS modules by using the `ifconfig interface modlist` command. For example, here is the `ifconfig` output for an `hme0` interface:

```
# ifconfig hme0 modlist
0 arp
1 ip
2 hme
```

Interfaces normally exist as network drivers directly below the IP module, as shown in the output from `ifconfig hme0 modlist`. They should not require additional configuration.

However, certain technologies, such as NCA or IP Filter, insert themselves as STREAMS modules between the IP module and the network driver. Problems can result in the way interfaces of the same IPMP group behave.

If a STREAMS module is stateful, then unexpected behavior can occur on failover, even if you push the same module onto all of the interfaces in a group. However, you can use stateless STREAMS modules, provided that you push them in the same order on all interfaces in the IPMP group.

b. Push the modules of an interface in the standard order for the IPMP group.

```
ifconfig interface modinsert module-name

ifconfig hme0 modinsert ip
```

5. Use the same IP addressing format on all interfaces of the IPMP group.

If one interface is configured for IPv4, then all interfaces of the group must be configured for IPv4. Suppose you have an IPMP group that is composed of

interfaces from several NICs. If you add IPv6 addressing to the interfaces of one NIC, then all interfaces in the IPMP group must be configured for IPv6 support.

6. Check that all interfaces in the IPMP group are connected to the same IP link.

7. Verify that the IPMP group does not contain interfaces with different network media types.

The interfaces that are grouped together should be of the same interface type, as defined in `/usr/include/net/if_types.h`. For example, you cannot combine Ethernet and Token ring interfaces in an IPMP group. As another example, you cannot combine a Token bus interface with asynchronous transfer mode (ATM) interfaces in the same IPMP group.

8. For IPMP with ATM interfaces, configure the ATM interfaces in LAN emulation mode.

IPMP is not supported for interfaces using Classical IP over ATM.

▼ SPARC: How to Ensure That the MAC Address of an Interface Is Unique

Before you configure an IPMP group, you must verify that every interface in the prospective group has a unique MAC address. Almost all interfaces come configured with a factory-set unique MAC address. However, every SPARC-based system has a system-wide MAC address, which by default is used by all interfaces. In an IPMP group, each interface must have a unique MAC address. Therefore, you must ensure that the EEPROM parameter `local-mac-address?` is set to `true` so that the interfaces use their factory-set MAC addresses. You can use the `eeprom` command to check the current value of `local-mac-address?` and change it, if necessary.

Steps 1. On the system with the interfaces to be configured, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Determine whether all interfaces on the system currently use the system-wide MAC address.

```
# eeprom local-mac-address?  
local-mac-address?=false
```

In the example, the value of `local-mac-address?=false` indicates that all interfaces do use the system-wide MAC address. The value of `local-mac-address?=false` must be changed to `true` before the interfaces can become members of an IPMP group.

3. If necessary, change the value of `local-mac-address?` as follows:

```
# eeprom local-mac-address?=true
```

When you reboot the system, the interfaces with factory-set MAC addresses instead use these factory settings. Interfaces without factory-set MAC addresses continue to use the system-wide MAC address.

4. Check the MAC addresses of the interfaces on the system.

```
ifconfig -a
lo0: flags=1000849 <UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.112 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:0:0:1
hme1: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.114 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:0:0:1
ge0: flags=1004843 <UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 10.0.0.118 netmask ffffffff broadcast 10.0.0.127
    ether 8:0:20:1:1:1
```

Look for cases where multiple interfaces have the same MAC address. In the previous example, `hme0` and `hme1` both have the same MAC address.

Note – Continue to the next step only if more than one network interface still has the same MAC address.

5. If necessary, manually configure the remaining interfaces so that all interfaces have unique MAC addresses.

Place a unique MAC address in the `/etc/hostname.interface` for the particular interface.

Note – To prevent any risk of manually configured MAC addresses conflicting with other MAC addresses on your network, you must always configure *locally administered* MAC addresses, as defined by the IEEE 802.3 standard.

In the previous example, you must configure either `hme0` or `hme1` with a locally-administered MAC address. For example, to reconfigure `hme1` with the locally-administered MAC address `06:05:04:03:02`, you would add the following line to `/etc/hostname.hme1`:

```
ether 06:05:04:03:02
```

You also can use the `ifconfig ether` command to configure an interface's MAC address for the current session. However, any changes made directly with `ifconfig` are not preserved across reboots. Refer to the `ifconfig(1M)` man page for details.

6. Reboot the system.

Configuring IPMP Groups

This section contains configuration tasks for a typical IPMP group with at least two physical interfaces.

- For an introduction to multiple interface IPMP groups, refer to “IPMP Group” on page 639.
- For planning tasks, refer to “Planning for an IPMP Group” on page 655.
- To configure an IPMP group with only one physical interface, refer to “Configuring IPMP Groups With a Single Physical Interface” on page 667.

▼ How to Configure an IPMP Group With Multiple Interfaces

Before You Begin You need to have already configured the IPv4 addresses, and, if appropriate, the IPv6 addresses of all interfaces in the prospective IPMP group.

Steps 1. On the system with the interfaces to be configured, assume the Primary Administrator role, or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Place each physical interface into an IPMP group.

```
# ifconfig interface group group-name
```

For example, to place hme0 and hme1 under group testgroup1, you would type the following commands:

```
# ifconfig hme0 group testgroup1
# ifconfig hme1 group testgroup1
```

Avoid using spaces in group names. The `ifconfig` status display does not show spaces. Consequently, do not create two similar group names where the only difference is that one name also contains a space. If one of the group names contains a space, these group names look the same in the status display.

In a dual-stack environment, placing the IPv4 instance of an interface under a particular group automatically places the IPv6 instance under the same group.

3. (Optional) Configure an IPv4 test address on one or more physical interfaces.

You need to configure a test address only if you want to use probe-based failure detection on a particular interface. Test addresses are configured as logical interfaces of the physical interface that you specify to the `ifconfig` command.

If one interface in the group is to become the standby interface, do not configure a test address for that interface at this time. You configure a test address for the standby interface as part of the task [“How to Configure a Standby Interface for an IPMP Group”](#) on page 665.

Use the following syntax of the `ifconfig` command for configuring a test address:

```
# ifconfig interface addif ip-address <parameters> -failover deprecated up
```

For example, you would create the following test address for the primary network interface `hme0`:

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

This command sets the following parameters for the primary network interface `hme0`:

- Address set to `192.168.85.21`
- Netmask and broadcast address set to the default value
- `-failover` and `deprecated` options set

Note – You must mark an IPv4 test address as deprecated to prevent applications from using the test address.

4. Check the IPv4 configuration for a specific interface.

You can always view the current status of an interface by typing `ifconfig interface`. For more information on viewing an interface’s status, refer to [“How to Get Information About a Specific Interface”](#) on page 153.

You can get information about test address configuration for a physical interface by specifying the logical interface that is assigned to the test address.

```
# ifconfig hme0:1
hme0:1: flags=9000843<UP, BROADCAST, RUNNING, MULTICAST, DEPRECATED, IPv4, NOFAILOVER>
mtu 1500 index 2
inet 192.168.85.21 netmask ffffffff broadcast 192.168.85.255
```

5. (Optional) If applicable, configure an IPv6 test address.

```
# ifconfig interface inet6 -failover
```

Physical interfaces with IPv6 addresses are placed into the same IPMP group as the interfaces’ IPv4 addresses. This happens when you configure the physical interface with IPv4 addresses into an IPMP group. If you first place physical interfaces with IPv6 addresses into an IPMP group, physical interfaces with IPv4 addresses are also implicitly placed in the same IPMP group.

For example, to configure `hme0` with an IPv6 test address, you would type the following:

```
# ifconfig hme0 inet6 -failover
```

You do not need to mark an IPv6 test address as deprecated to prevent applications from using the test address.

6. Check the IPv6 configuration.

```
# ifconfig hme0 inet6
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6,NOFAILOVER> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:17fa/10
      groupname test
```

The IPv6 test address is the link-local address of the interface.

7. (Optional) Preserve the IPMP group configuration across reboots.

- For IPv4, add the following line to the `/etc/hostname.interface` file:

```
interface-address <parameters> group group-name up \
      addif logical-interface -failover deprecated <parameters> up
```

In this instance, the test IPv4 address is configured only on the next reboot. If you want the configuration to be invoked in the current session, do steps 1, 2, and, optionally 3.

- For IPv6, add the following line to the `/etc/hostname6.interface` file:

```
-failover group group-name up
```

This test IPv6 address is configured only on the next reboot. If you want the configuration to be invoked in the current session, do steps 1, 2, and, optionally, 5.

8. (Optional) Add more interfaces to the IPMP group by repeating steps 1 through 6.

You can add new interfaces to an existing group on a live system. However, changes are lost across reboots.

Example 30–1 Configuring an IPMP Group With Two Interfaces

Suppose you want to do the following:

- Have the netmask and broadcast address set to the default value.
- Configure the interface with a test address 192.168.85.21.

You would type the following command:

```
# ifconfig hme0 addif 192.168.85.21 netmask + broadcast + -failover deprecated up
```

You must mark an IPv4 test address as deprecated to prevent applications from using the test address. See [“How to Configure an IPMP Group With Multiple Interfaces”](#) on page 659.

To turn on the failover attribute of the address, you would use the `failover` option without the dash

All test IP addresses in an IPMP group must use the same network prefix. The test IP addresses must belong to a single IP subnet.

Example 30–2 Preserving an IPv4 IPMP Group Configuration Across Reboots

Suppose you want to create an IPMP group called `testgroup1` with the following configuration:

- Physical interface `hme0` with address `192.168.85.19`
- A logical interface address of `192.168.85.21`
- `deprecated` and `-failover` options set
- Netmask and broadcast address set to the default value

You would add the following line to the `/etc/hostname.hme0` file:

```
192.168.85.19 netmask + broadcast + group testgroup1 up \  
    addif 192.168.85.21 deprecated -failover netmask + broadcast + up
```

Similarly, to place the second interface `hme1` under the same group `testgroup1` and to configure a test address, you would add the following line:

```
192.168.85.20 netmask + broadcast + group test up \  
    addif 192.168.85.22 deprecated -failover netmask + broadcast + up
```

Example 30–3 Preserving an IPv6 IPMP Group Configuration Across Reboots

To create a test group for interface `hme0` with an IPv6 address, you would add the following line to the `/etc/hostname6.hme0` file:

```
-failover group testgroup1 up
```

Similarly, to place the second interface `hme1` in group `testgroup1` and to configure a test address, you would add the following line to the `/etc/hostname6.hme1` file:

```
-failover group test up
```

Troubleshooting During IPMP group configuration, `in.mpathd` outputs a number of messages to the system console or to the `syslog` file. These messages are informational in nature and indicate that the IPMP configuration functions correctly.

- This message indicates that interface `hme0` was added to IPMP group `testgroup1`. However, `hme0` does not have a test address configured. To enable probe-based failure detection, you need to assign a test address to the interface.

```
May 24 14:09:57 host1 in.mpathd[101180]: No test address configured on interface hme0;  
disabling probe-based failure detection on it.  
testgroup1
```

- This message appears for all interfaces with only IPv4 addresses that are added to an IPMP group.

```
May 24 14:10:42 host4 in.mpathd[101180]: NIC qfe0 of group testgroup1 is not  
plumbed for IPv6 and may affect failover capability
```

- This message should appear when you have configured a test address for an interface.

```
Created new logical interface hme0:1
May 24 14:16:53 host1 in.mpathd[101180]: Test address now configured on interface hme0;
enabling probe-based failure detection on it
```

See Also If you want the IPMP group to have an active-standby configuration, go on to [“How to Configure a Standby Interface for an IPMP Group”](#) on page 665.

Configuring Target Systems

Probe-based failure detection involves the use of target systems, as explained in [“Probe-Based Failure Detection”](#) on page 647. For some IPMP groups, the default targets used by `in.mpathd` is sufficient. However, for some IPMP groups, you might want to configure specific targets for probe-based failure detection. You accomplish probe-based failure detection by setting up host routes in the routing table as probe targets. Any host routes that are configured in the routing table are listed before the default router. Therefore, IPMP uses the explicitly defined host routes for target selection. You can use either of two methods for directly specifying targets: manually setting host routes or creating a shell script that can become a startup script.

Consider the following criteria when evaluating which hosts on your network might make good targets.

- Make sure that the prospective targets are available and running. Make a list of their IP addresses.
- Ensure that the target interfaces are on the same network as the IPMP group that you are configuring.
- The netmask and broadcast address of the target systems must be the same as the addresses in the IPMP group.
- The target host must be able to answer ICMP requests from the interface that is using probe-based failure detection.

▼ How to Manually Specify Target Systems for Probe-Based Failure Detection

- Steps**
1. Log in with your user account to the system where you are configuring probe-based failure detection.
 2. Add a route to a particular host to be used as a target in probe-based failure detection.

```
$ route add -host destination-IP gateway-IP -static
```

Replace the values of *destination-IP* and *gateway-IP* with the IPv4 address of the host to be used as a target. For example, you would type the following to specify the target system 192.168.85.137, which is on the same subnet as the interfaces in IPMP group testgroup1.

```
$ route add -host 192.168.85.137 192.168.85.137 -static
```

3. Add routes to additional hosts on the network to be used as target systems.

▼ How to Specify Target Systems in a Shell Script

- Steps**
1. On the system where you have configured an IPMP group, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Create a shell script that sets up static routes to your proposed targets.

For example, you could create a shell script called `ipmp.targets` with the following contents:

```
TARGETS="192.168.85.117 192.168.85.127 192.168.85.137"

case "$1" in
  'start')
    /usr/bin/echo "Adding static routes for use as IPMP targets"
    for target in $TARGETS; do
      /usr/sbin/route add -host $target $target
    done
    ;;
  'stop')
    /usr/bin/echo "Removing static routes for use as IPMP targets"
    for target in $TARGETS; do
      /usr/sbin/route delete -host $target $target
    done
    ;;
esac
```

3. Copy the shell script to the startup script directory.

```
# cp ipmp.targets /etc/init.d
```

4. Change the permissions on the new startup script.

```
# chmod 744 /etc/init.d/ipmp.targets
```

5. Change ownership of the new startup script.

```
# chown root:sys /etc/init.d/ipmp.targets
```


6. Create a link for the startup script in the `/etc/init.d` directory.

```
# ln /etc/init.d/ipmp.targets /etc/rc2.d/S70ipmp.targets
```

The `S70` prefix in the file name `S70ipmp.targets` orders the new script properly with respect to other startup scripts.

Configuring Standby Interfaces

Use this procedure if you want the IPMP group to have an active-standby configuration. For more information on this type of configuration, refer to [“IPMP Interface Configurations” on page 644](#).

▼ How to Configure a Standby Interface for an IPMP Group

Before You Begin

- You must have configured all interfaces as members of the IPMP group.
- You should not have configured a test address on the interface to become the standby interface.

For information on configuring an IPMP group and assigning test addresses, refer to [“How to Configure an IPMP Group With Multiple Interfaces” on page 659](#).

Steps 1. **On the system with the standby interfaces to be configured, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Configure an interface as a standby and assign the test address.**

```
# ifconfig interface plumb ip-address <other-parameters> deprecated -failover standby up
```

A standby interface can have only one IP address, the test address. You must set the `-failover` option before you set the `standby up` option. For `<other-parameters>`, use the parameters that are required by your configuration, as described in the `ifconfig(1M)` man page.

- For example, to create an IPv4 test address, you would type the following command:

```
# ifconfig hme1 plumb 192.168.85.22 netmask + broadcast + deprecated -failover standby up
```

<code>hme1</code>	Defines <code>hme1</code> as the physical interface to be configured as the standby interface.
<code>192.168.85.22</code>	Assigns this test address to the standby interface.
<code>deprecated</code>	Indicates that the test address is not used for outbound packets.

-failover Indicates that the test address does not fail over if the interface fails.

standby Marks the interface as a standby interface.

- For example, to create an IPv6 test address, you would type the following command:

```
# ifconfig hme1 plumb -failover standby up
```

3. Check the results of the standby interface configuration.

```
# ifconfig hme1
hme1: flags=69040843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER,
STANDBY,INACTIVE mtu 1500
    index 4 inet 192.168.85.22 netmask ffffffff broadcast 19.16.85.255
    groupname test
```

The `INACTIVE` flag indicates that this interface is not used for any outbound packets. When a failover occurs on this standby interface, the `INACTIVE` flag is cleared.

Note – You can always view the current status of an interface by typing the `ifconfig interface` command. For more information on viewing interface status, refer to [“How to Get Information About a Specific Interface”](#) on page 153.

4. (Optional) Preserve the IPv4 standby interface across reboots.

Assign the standby interface to the same IPMP group, and configure a test address for the standby interface.

For example, to configure `hme1` as the standby interface, you would add the following line to the `/etc/hostname.hme1` file:

```
192.168.85.22 netmask + broadcast + deprecated group test -failover standby up
```

5. (Optional) Preserve the IPv6 standby interface across reboots.

Assign the standby interface to the same IPMP group, and configure a test address for the standby interface.

For example, to configure `hme1` as the standby interface, add the following line to the `/etc/hostname6.hme1` file:

```
-failover group test standby up
```

Example 30–4 Configuring a Standby Interface for an IPMP Group

Suppose you want to create a test address with the following configuration:

- Physical interface `hme2` as a standby interface
- Test address of `192.168.85.22`
- `deprecated` and `-failover` options set

- Netmask and broadcast address set to the default value

You would type the following:

```
# ifconfig hme2 plumb 192.168.85.22 netmask + broadcast + deprecated -failover standby up
```

The interface is marked as a standby interface only after the address is marked as a NOFAILOVER address.

You would remove the standby status of an interface by typing the following:

```
# ifconfig interface -standby
```

Configuring IPMP Groups With a Single Physical Interface

When you have only one interface in an IPMP group, failover is not possible. However, you can enable failure detection on that interface by assigning the interface to an IPMP group. You do not have to configure a dedicated test IP address to establish failure detection for a single interface IPMP group. You can use a single IP address for sending data and detecting failure.

▼ How to Configure a Single Interface IPMP Group

- Steps**
1. **On the system with the prospective single interface IPMP group, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **For IPv4, create the single interface IPMP group.**

You can use either of the following methods:

- Use the following syntax to assign the single interface to an IPMP group.

```
# ifconfig interface -failover group group-name
```

The following example assigns the interface hme0 into the IPMP group v4test:

```
# ifconfig hme0 -failover group v4test
```

Unlike the multiple physical interface configuration, you would not mark a single physical interface as deprecated.

This example includes the use of the `-failover` option of the `ifconfig` command to create an `IFF_NOFAILOVER` flag for the interface. Consider using `-failover` if you might later add more interfaces to the group. The `in.mpathd` daemon sends probe packets by using that address. Later, when you add more interfaces, the configuration should work properly.

- Alternatively, you can use the following syntax to add a single physical interface to an IPMP group:

```
# ifconfig interface group group-name
```

When you use this configuration, `in.mpathd` chooses a data address to send probe packets.

3. For IPv6, create the single interface IPMP group.

Use either of the following two methods:

- Use the following syntax to assign the single interface to an IPMP group:

```
# ifconfig interface inet6 -failover group group-name
```

For example, you would type the following to add the single interface `hme0` into the IPMP group `v6test`:

```
# ifconfig hme0 inet6 -failover group v6test
```

- Use the following syntax if you do not want to set the `NOFAILOVER` flag:

```
# ifconfig interface inet6 group group-name
```

When the `in.mpathd` daemon detects failures, the interface is marked and logged appropriately on the console.

In a single physical interface configuration, you cannot verify whether the target system that is being probed has failed or whether the interface has failed. The target system can be probed through only one physical interface. If only one default router is on the subnet, turn off IPMP if a single physical interface is in the group. If a separate IPv4 and IPv6 default router exists, or multiple default routers exist, more than one target system needs to be probed. Hence, you can safely turn on IPMP.

Maintaining IPMP Groups

This section contains tasks for maintaining existing IPMP groups and the interfaces that compose those groups. The tasks presume that you have already configured an IPMP group, as explained in [“Configuring IPMP Groups” on page 655](#).

▼ How to Display the IPMP Group Membership of an Interface

- Steps**
1. **On the system with the IPMP group configuration, become superuser or assume an equivalent role.**

Roles contain authorizations and privileged commands. For more information about roles, see “Configuring RBAC (Task Map)” in *System Administration Guide: Security Services*.

2. **Display information about the interface, including the group to which the interface belongs.**

```
# ifconfig interface
```

3. **If applicable, display IPv6 information for the interface.**

```
# ifconfig interface inet6
```

Example 30–5 Displaying Physical Interface Groups

To display the group name for hme0, you would type the following:

```
# ifconfig hme0
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
      index 2 inet 192.168.85.19 netmask ffffffff broadcast 192.168.85.255
      groupname testgroup1
```

To display the group name for only the IPv6 information, you would type the following:

```
# ifconfig hme0 inet6
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
      inet6 fe80::a00:20ff:feb9:19fa/10
      groupname testgroup1
```

▼ How to Add an Interface to an IPMP Group

- Steps**
1. **On the system with the IPMP group configuration, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Add the interface to the IPMP group.

```
# ifconfig interface group group-name
```

The interface specified in *interface* becomes a member of IPMP group *group-name*.

Example 30–6 Adding an Interface to an IPMP Group

To add `hme0` to the IPMP group `test`, you would type the following command:

```
# ifconfig hme0 group testgroup2
hme0: flags=9000843<UP ,BROADCAST,RUNNING,MULTICAST,IPv4,NOFAILOVER> mtu 1500 index 2
inet 192.168.85.19 netmask ff000000 broadcast 10.255.255.255
groupname testgroup2
ether 8:0:20:c1:8b:c3
```

▼ How to Remove an Interface From an IPMP Group

When you execute the `ifconfig` command's `group` parameter with a null string, the interface is removed from its current IPMP group. Be careful when removing interfaces from a group. If some other interface in the IPMP group has failed, a failover could have happened earlier. For example, if `hme0` failed previously, all addresses are failed over to `hme1`, if `hme1` is part of the same group. The removal of `hme1` from the group causes the `in.mpathd` daemon to return all the failover addresses to some other interface in the group. If no other interfaces are functioning in the group, failover might not restore all the network accesses.

Similarly, when an interface in a group needs to be unplumbed, you should first remove the interface from the group. Then, ensure that the interface has all the original IP addresses configured. The `in.mpathd` daemon tries to restore the original configuration of an interface that is removed from the group. You need to ensure that the configuration is restored before unplumbing the interface. Refer to [“What Happens During Interface Failover”](#) on page 648 to see how interfaces look before and after a failover.

Steps 1. On the system with the IPMP group configuration, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Remove the interface from the IPMP group.

```
# ifconfig interface group ""
```

The quotation marks indicate a null string.

Example 30–7 Removing an Interface From a Group

To remove `hme0` from the IPMP group `test`, you would type the following command:

```
# ifconfig hme0 group ""
# ifconfig hme0
hme0: flags=9000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 2 inet 192.168.85.19 netmask ffffffff broadcast 192.168.85.255
# ifconfig hme0 inet6
hme0: flags=a000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
inet6 fe80::a00:20ff:feb9:19fa/10
```

▼ How to Move an Interface From One IPMP Group to Another Group

You can place an interface in a new IPMP group when the interface belongs to an existing IPMP group. You do not need to remove the interface from the current IPMP group. When you place the interface in a new group, the interface is automatically removed from any existing IPMP group.

Steps 1. On the system with the IPMP group configuration, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Move the interface to a new IPMP group.

```
# ifconfig interface group group-name
```

Placing the interface in a new group automatically removes the interface from any existing group.

Example 30–8 Moving an Interface to a Different IPMP Group

To change the IPMP group of interface `hme0`, you would type the following:

```
# ifconfig hme0 group cs-link
```

This command removes the `hme0` interface from IPMP group `test` and then puts the interface in the group `cs-link`.

Replacing a Failed Physical Interface on Systems That Support Dynamic Reconfiguration

This section contains procedures that relate to administering systems that support dynamic reconfiguration (DR).

Note – The tasks pertain only to IP layers that are configured by using the `ifconfig` command. Layers before or after the IP layer, such as ATM or other services, require specific manual steps if the layers are not automated. The steps in the next procedures are used to unconfigure interfaces during predetachment and configure interface after postattachment.

▼ How to Remove a Physical Interface That Has Failed (DR-Detach)

This procedure shows how to remove a physical interface on a system that supports DR. The procedure assumes that the following conditions already exist:

- Physical interfaces `hme0` and `hme1` are the example interfaces.
- Both interfaces are in the same IPMP group.
- `hme0` has failed.
- Logical interface `hme0:1` has the test address.
- You are replacing the failed interface with the same physical interface name, for example, `hme0` with `hme0`.

Note – You can skip Step 2 if the test address is plumbed by using the `/etc/hostname.hme0` file.

Steps 1. **On the system with the IPMP group configuration, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Display the test address configuration.

```
# ifconfig hme0:1

hme0:1:
flags=9040842<BROADCAST, RUNNING, MULTICAST, DEPRECATED, IPv4, NOFAILOVER>
mtu 1500 index 3
inet 192.168.233.250 netmask ffffffff broadcast 192.168.233.255
```

You need this information to replumb the test address when replacing the physical interface.

3. Remove the physical interface.

Refer to the following sources for a complete description of how to remove the physical interface:

- `cfgadm(1M)` man page
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide*

▼ How to Replace a Physical Interface That Has Failed (DR-Attach)

This procedure shows how to replace a physical interface on a system that supports DR.

Steps 1. On the system with the IPMP group configuration, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Replace the physical interface.

Refer to the instructions in the following sources:

- `cfgadm(1M)` man page
- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*
- *Sun Enterprise 10000 DR Configuration Guide*, or *Sun Fire 880 Dynamic Reconfiguration User's Guide*

3. Plumb and bring up the test address.

```
# ifconfig hme0 test-address-configuration
```

Use the same test address configuration that was configured in the `/etc/hostname.hme0` file. The test configuration is the same configuration that is displayed in Step 2 in the procedure [“How to Remove a Physical Interface That Has Failed \(DR-Detach\)”](#) on page 672.

This configuration triggers the `in.mpathd` daemon to resume probing. As a result of this probing, `in.mpathd` detects the repair. Consequently, `in.mpathd` causes the original IP address to fail back from `hme1`.

See [“Test Addresses”](#) on page 642 for more details about test addresses.

Note – The failback of IP addresses during the recovery of a failed physical interface takes up to three minutes. This time might vary, depending on network traffic. The time also depends on the stability of the incoming interface to fail back the failed-over interfaces by the `in.mpathd` daemon.

Recovering a Physical Interface That Was Not Present at System Boot

Note – The following procedure pertains only to IP layers that are configured by using the `ifconfig` command. Layers before or after the IP layer, such as ATM or other services, require specific manual steps if the layers are not automated. The specific steps in the next procedure are used to unconfigure interfaces during predetachment and to configure interfaces after postattachment.

Recovery after dynamic reconfiguration is automatic for an interface that is part of the I/O board on a Sun Fire™ platform. If the NIC is a Sun Crypto Accelerator I - cPCI board, the recovery is also automatic. Consequently, the following steps are not required for an interface that is coming back as part of a DR operation. For more information on the Sun Fire x800 and Sun Fire 15000 systems, see the `cfgadm_sbd(1M)` man page. The physical interface fails back to the configuration that is specified in the `/etc/hostname.interface` file. See [“Configuring IPMP Groups”](#) on page 655 for details on how to configure interfaces to preserve the configuration across reboots.

Note – On Sun Fire legacy (Exx00) systems, DR detachments are still subject to manual procedures. However, DR attachments are automated.

▼ How to Recover a Physical Interface That Was Not Present at System Boot

You must complete the following procedure before you recover a physical interface that was not present at system boot. The example in this procedure has the following configuration:

- Physical interfaces hme0 and hme1 are the interfaces.
- Both interfaces are in the same IPMP group.
- hme0 was not installed at system boot.

Note – The failback of IP addresses during the recovery of a failed physical interface takes up to three minutes. This time might vary, depending on network traffic. The time also depends on the stability of the incoming interface to fail back the failed-over interfaces by the `in.mpathd` daemon.

Steps 1. On the system with the IPMP group configuration, assume the Primary Administrator role or become superuser.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Retrieve the failed network information from the failure error message of the console log.

See the `syslog(3C)` man page. The error message might be similar to the following:

```
moving addresses from failed IPv4 interfaces:  
hme1 (moved to hme0)
```

This message indicates that the IPv4 addresses on the failed interface hme1 have failed over to the hme0 interface.

Alternatively, you might receive the following similar message:

```
moving addresses from failed IPv4 interfaces:  
hme1 (couldn't move, no alternative interface)
```

This message indicates that no active interface could be found in the same group as failed interface hme1. Therefore, the IPv4 addresses on hme1 could not fail over.

3. Attach the physical interface to the system.

Refer to the following for instructions on how to replace the physical interface:

- `cfgadm(1M)` man page
- *Sun Enterprise 10000 DR Configuration Guide*

- *Sun Enterprise 6x00, 5x00, 4x00, and 3x00 Systems Dynamic Reconfiguration User's Guide*

4. Refer to the message content from Step 2. If the addresses could not be moved, go to Step 6. If the addresses were moved, continue to Step 5.
5. Unplumb the logical interfaces that were configured as part of the failover process.
 - a. Review the contents of the `/etc/hostname.moved-from-interface` file to determine what logical interfaces were configured as part of the failover process.
 - b. Unplumb each failover IP address.

```
# ifconfig moved-to-interface removeif moved-ip-address
```

Note – Failover addresses are marked with the `failover` parameter, or are not marked with the `-failover` parameter. You do not need to unplumb IP addresses that are marked `-failover`.

For example, assume that the contents of the `/etc/hostname.hme0` file contains the following lines:

```
inet 10.0.0.4 -failover up group one
addif 10.0.0.5 failover up
addif 10.0.0.6 failover up
```

To unplumb each failover IP address, you would type the following commands:

```
# ifconfig hme0 removeif 10.0.0.5
# ifconfig hme0 removeif 10.0.0.6
```

6. Reconfigure the IPv4 information for the replaced physical interface by typing the following command for each interface that was removed:

```
# ifconfig removed-from-NIC <parameters>
```

For example, you would type the following commands:

```
# ifconfig hme1 inet plumb
# ifconfig hme1 inet 10.0.0.4 -failover up group one
# ifconfig hme1 addif 10.0.0.5 failover up
# ifconfig hme1 addif 10.0.0.6 failover up
```

Modifying the `/etc/default/mpathd` IPMP Configuration File

The IPMP configuration file `/etc/default/mpathd` contains three parameters that you can modify for your configuration requirements:

- `FAILURE_DETECTION_TIME`
- `FAILBACK`
- `TRACK_INTERFACES_ONLY_WITH_GROUPS`

▼ How to Configure the `/etc/default/mpathd` File

- Steps**
1. **On the system with the IPMP group configuration, assume the Primary Administrator role or become superuser.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Edit the `/etc/default/mpathd` file.**

Change the default value of one or more of the three parameters.

- a. **Type the new value for the `FAILURE_DETECTION_TIME` parameter.**

```
FAILURE_DETECTION_TIME=n
```

where *n* is the amount of time in seconds for ICMP probes to detect whether an interface failure has occurred. The default is 10 seconds.

- b. **Type the new value for the `FAILBACK` parameter.**

```
FAILBACK=[yes | no]
```

- c. **Type the new value for the `TRACK_INTERFACES_ONLY_WITH_GROUPS` parameter.**

```
TRACK_INTERFACES_ONLY_WITH_GROUPS=[yes | no]
```

3. **Restart the `in.mpathd` daemon.**

```
# pkill -HUP in.mpathd
```


PART **VII** IP Quality of Service (IPQoS)

This part contains tasks and information about IP Quality of Service (IPQoS), the Solaris operating system's implementation of differentiated services.

Introducing IPQoS (Overview)

IP Quality of Service (IPQoS) enables you to prioritize, control, and gather accounting statistics. Using IPQoS, you can provide consistent levels of service to users of your network. You can also manage traffic to avoid network congestion.

The following is a list of topics in this chapter:

- “IPQoS Basics” on page 681
- “Providing Quality of Service With IPQoS” on page 684
- “Improving Network Efficiency With IPQoS” on page 685
- “Differentiated Services Model” on page 687
- “Traffic Forwarding on an IPQoS-Enabled Network” on page 691

IPQoS Basics

IPQoS enables the Differentiated Services (Diffserv) architecture that is defined by the Differentiated Services Working Group of the Internet Engineering Task Force (IETF). In the Solaris OS, IPQoS is implemented at the IP level of the TCP/IP protocol stack.

What Are Differentiated Services?

By enabling IPQoS, you can provide different levels of network service for selected customers and selected applications. The different levels of service are collectively referred to as *differentiated services*. The differentiated services that you provide to customers can be based on a structure of service levels that your company offers to its customers. You can also provide differentiated services based on the priorities that are set for applications or users on your network.

Providing quality of service involves the following activities:

- Delegating levels of service to different groups, such as customers or departments in an enterprise
- Prioritizing network services that are given to particular groups or applications
- Discovering and eliminating areas of network bottlenecks and other forms of congestion
- Monitoring network performance and providing performance statistics
- Regulating bandwidth to and from network resources

IPQoS Features

IPQoS has the following features:

- `ipqosconf` Command-line tool for configuring the QoS policy
- Classifier that selects actions, which are based on filters that configure the QoS policy of your organization
- Metering module that measures network traffic, in compliance with the Diffserv model
- Service differentiation that is based on the ability to mark a packet's IP header with forwarding information
- Flow-accounting module that gathers statistics for traffic flows
- Statistics gathering for traffic classes, through the UNIX® `kstat` command
- Support for SPARC® architecture
- Support for IPv4 and IPv6 addressing
- Interoperability with IP Security Architecture (IPsec)
- Support for 802.1D user-priority markings for virtual local area networks (VLANs)

Where to Get More Information About Quality-of-Service Theory and Practice

You can find information on differentiated services and quality of service from print and online sources.

Books About Quality of Service

For more information on quality-of-service theory and practice, refer to the following books:

- Ferguson, Paul and Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

Requests for Comments (RFCs) About Quality of Service

IPQoS conforms to the specifications that are described in the following RFCs and the following Internet drafts:

- RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (<http://www.ietf.org/rfc/rfc2474.txt?number=2474>) – Describes an enhancement to the type of service (ToS) field or DS fields of the IPv4 and IPv6 packet headers to support differentiated services
- RFC 2475, An Architecture for Differentiated Services (<http://www.ietf.org/rfc/rfc2475.txt?number=2475>) – Provides a detailed description of the organization and modules of the Diffserv architecture
- RFC 2597, Assured Forwarding PHB Group (<http://www.ietf.org/rfc/rfc2597.txt?number=2597>) – Describes how the assured forwarding (AF) per-hop behavior works.
- RFC 2598, An Expedited Forwarding PHB (<http://www.ietf.org/rfc/rfc2598.txt?number=2598>) – Describes how the expedited forwarding (EF) per-hop behavior works
- Internet-Draft, *An Informal Management Model for Diffserv Routers* – Presents a model for implementing the Diffserv architecture on routers.

Web Sites With Quality-of-Service Information

The Differentiated Services Working Group of the IETF maintains a web site with links to Diffserv Internet drafts at

<http://www.ietf.org/html.charters/diffserv-charter.html>.

Router manufacturers such as Cisco Systems and Juniper Networks provide information on their corporate web sites that describes how Differentiated Services are implemented in their products.

IPQoS Man Pages

IPQoS documentation includes the following man pages:

- `ipqosconf(1M)` - Describes the command for setting up the IPQoS configuration file
- `ipqos(7ipp)` – Describes the IPQoS implementation of the Diffserv architectural model
- `ipgpc(7ipp)` – Describes the IPQoS implementation of a Diffserv classifier
- `tokenmt(7ipp)` – Describes the IPQoS tokenmt meter
- `tswtclmt(7ipp)` – Describes the IPQoS `tswtclmt` meter
- `dscpmk(7ipp)` – Describes the DSCP marker module
- `dlcosmk(7ipp)` – Describes the IPQoS 802.1D user-priority marker module

- `flowacct(7ipp)`– Describes the IPQoS flow-accounting module
- `acctadm(1M)` – Describes the command that configures the Solaris extended accounting facilities. The `acctadm` command includes IPQoS extensions.

Providing Quality of Service With IPQoS

IPQoS features enable Internet service providers (ISPs) and application service providers (ASPs) to offer different levels of network service to customers. These features enable individual companies and educational institutions to prioritize services for internal organizations or for major applications.

Implementing Service-Level Agreements

If your organization is an ISP or ASP, you can base your IPQoS configuration on the *service-level agreement* (SLA) that your company offers to its customers. In an SLA, a service provider guarantees to a customer a certain level of network service that is based on a price structure. For example, a premium-priced SLA might ensure that the customer receives highest priority for all types of network traffic 24 hours per day. Conversely, a medium-priced SLA might guarantee that the customer receives high priority for email only during business hours. All other traffic would receive medium priority 24 hours a day.

Assuring Quality of Service for an Individual Organization

If your organization is an enterprise or an institution, you can also provide quality-of-service features for your network. You can guarantee that traffic from a particular group or from a certain application is assured a higher or lower degree of service.

Introducing the Quality-of-Service Policy

You implement quality of service by defining a *quality-of-service (QoS) policy*. The QoS policy defines various network attributes, such as customers' or applications' priorities, and actions for handling different categories of traffic. You implement your organization's QoS policy in an IPQoS configuration file. This file configures the IPQoS modules that reside in the Solaris OS kernel. A host with an applied IPQoS policy is considered an *IPQoS-enabled system*.

Your QoS policy typically defines the following:

- Discrete groups of network traffic that are called *classes of service*.
- Metrics for regulating the amount of network traffic for each class. These metrics govern the traffic-measuring process that is called *metering*.
- An action that an IPQoS system and a Diffserv router must apply to a packet flow. This type of action is called a *per-hop behavior* (PHB).
- Any statistics gathering that your organization requires for a class of service. An example is traffic that is generated by a customer or particular application.

When packets pass to your network, the IPQoS-enabled system evaluates the packet headers. The action that the IPQoS system takes is determined by your QoS policy.

Tasks for designing the QoS policy are described in [“Planning the Quality-of-Service Policy” on page 699](#).

Improving Network Efficiency With IPQoS

IPQoS contains features that can help you make network performance more efficient as you implement quality of service. When computer networks expand, the need also increases for managing network traffic that is generated by increasing numbers of users and more powerful processors. Some symptoms of an overused network include lost data and traffic congestion. Both symptoms result in slow response times.

In the past, system administrators handled network traffic problems by adding more bandwidth. Often, the level of traffic on the links varied widely. With IPQoS, you can manage traffic on the existing network and help assess where, and whether, expansion is necessary.

For example, for an enterprise or institution, you must maintain an efficient network to avoid traffic bottlenecks. You must also ensure that a group or application does not consume more than its allotted bandwidth. For an ISP or ASP, you must manage network performance to ensure that customers receive their paid-for level of network service.

How Bandwidth Affects Network Traffic

You can use IPQoS to regulate network *bandwidth*, the maximum amount of data that a fully used network link or device can transfer. Your QoS policy should prioritize the use of bandwidth to provide quality of service to customers or users. The IPQoS metering modules enable you to measure and control bandwidth allocation among the various traffic classes on an IPQoS-enabled host.

Before you can effectively manage traffic on your network, you must answer these questions about bandwidth usage:

- What are the traffic problem areas for your local network?
- What must you do to achieve optimum use of available bandwidth?
- What are your site's critical applications, which must be given highest priority?
- Which applications are sensitive to congestion?
- What are your less critical applications, which can be given a lower priority?

Using Classes of Service to Prioritize Traffic

To implement quality of service, you analyze network traffic to determine any broad groupings into which the traffic can be divided. Then, you organize the various groupings into classes of service with individual characteristics and individual priorities. These classes form the basic categories on which you base the QoS policy for your organization. The classes of service represent the traffic groups that you want to control.

For example, a provider might offer platinum, gold, silver, and bronze levels of service, available at a sliding price structure. A platinum SLA might guarantee top priority to incoming traffic that is destined for a web site that the ISP hosts for the customer. Thus, incoming traffic to the customer's web site could be one traffic class.

For an enterprise, you could create classes of service that are based on department requirements. Or, you could create classes that are based on the preponderance of a particular application in the network traffic. Here are a few examples of traffic classes for an enterprise:

- Popular applications such as email and outgoing FTP to a particular server, either of which could constitute a class. Because employees constantly use these applications, your QoS policy might guarantee email and outgoing FTP a small amount of bandwidth and a lower priority.
- An order-entry database that needs to run 24 hours a day. Depending on the importance of the database application to the enterprise, you might give the database a large amount of bandwidth and a high priority.
- A department that performs critical work or sensitive work, such as the payroll department. The importance of the department to the organization would determine the priority and amount of bandwidth you would give to such a department.
- Incoming calls to a company's external web site. You might give this class a moderate amount of bandwidth that runs at low priority.

Differentiated Services Model

IPQoS includes the following modules, which are part of the *Differentiated Services (Diffserv)* architecture that is defined in RFC 2475:

- Classifier
- Meter
- Marker

IPQoS adds the following enhancements to the Diffserv model:

- Flow-accounting module
- 802.1D datagram marker

This section introduces the Diffserv modules as they are used by IPQoS. You need to know about these modules, their names, and their uses to set up the QoS policy. For detailed information about each module, refer to [“IPQoS Architecture and the Diffserv Model” on page 757](#).

Classifier (`ipgpc`) Overview

In the Diffserv model, the *classifier* selects packets from a network traffic flow. A *traffic flow* consists of a group of packets with identical information in the following IP header fields:

- Source address
- Destination address
- Source port
- Destination port
- Protocol number

In IPQoS, these fields are referred to as the *5-tuple*.

The IPQoS classifier module is named `ipgpc`. The `ipgpc` classifier arranges traffic flows into classes that are based on characteristics you configure in the IPQoS configuration file.

For detailed information about `ipgpc`, refer to [“Classifier Module” on page 758](#).

Classes

A *class* is a group of network flows that share similar characteristics. For example, an ISP might define classes to represent the different service levels that are offered to customers. An ASP might define SLAs that give different levels of service to various applications. For an ASP’s QoS policy, a class might include outgoing FTP traffic that is bound for a particular destination IP address. Outgoing traffic from a company’s external web site might also be defined as a class.

Grouping traffic into classes is a major part of planning your QoS policy. When you create classes by using the `ipqosconf` utility, you are actually configuring the `ipgpc` classifier.

For information on how to define classes, see [“How to Define the Classes for Your QoS Policy”](#) on page 702.

Filters

Filters are sets of rules that contain parameters called *selectors*. Each filter must point to a class. IPQoS matches packets against the selectors of each filter to determine if the packet belongs to the filter’s class. You can filter on a packet by using a variety of selectors, for example, the IPQoS 5-tuple and other common parameters:

- Source address and destination addresses
- Source port and destination port
- Protocol numbers
- User IDs
- Project IDs
- Differentiated Services Codepoint (DSCP)
- Interface index

For example, a simple filter might include the destination port with the value of 80. The `ipgpc` classifier then selects all packets that are bound for destination port 80 (HTTP) and handles the packets as directed in the QoS policy.

For information on creating filters, see [“How to Define Filters in the QoS Policy”](#) on page 705.

Meter (tokenmt and tswtclmt) Overview

In the Diffserv model, the *meter* tracks the transmission rate of traffic flows on a per-class basis. The meter evaluates how much the actual rate of the flow conforms to the configured rates to determine the appropriate outcome. Based on the traffic flow’s outcome, the meter selects a subsequent action. Subsequent actions might include sending the packet to another action or returning the packet to the network without further processing.

The IPQoS meters determine whether a network flow conforms to the transmission rate that is defined for its class in the QoS policy. IPQoS includes two metering modules:

- `tokenmt` – Uses a two-token bucket metering scheme
- `tswtclmt` – Uses a time-sliding window metering scheme

Both metering modules recognize three outcomes: red, yellow, and green. You define the actions to be taken for each outcome in the parameters `red_action_name`, `yellow_action_name`, and `green_action_name`.

In addition, you can configure `tokenmt` to be color aware. A color-aware metering instance uses the packet's size, DSCP, traffic rate, and configured parameters to determine the outcome. The meter uses the DSCP to map the packet's outcome to a green, yellow, or red.

For information on defining parameters for the IPQoS meters, refer to [“How to Plan Flow Control” on page 706](#).

Marker (`dscpmk` and `dlcosmk`) Overview

In the Diffserv model, the *marker* marks a packet with a value that reflects a forwarding behavior. *Marking* is the process of placing a value in the packet's header to indicate how to forward the packet to the network. IPQoS contains two marker modules:

- `dscpmk` – Marks the DS field in an IP packet header with a numeric value that is called the *Differentiated Services codepoint*, or *DSCP*. A Diffserv-aware router can then use the DS codepoint to apply the appropriate forwarding behavior to the packet.
- `dlcosmk` – Marks the virtual local area network (VLAN) tag of an Ethernet frame header with a numeric value that is called the *user priority*. The user priority indicates the *class of service (CoS)*, which defines the appropriate forwarding behavior to be applied to the datagram.

`dlcosmk` is an IPQoS addition that is not part of the Diffserv model, as designed by the IETF.

For information on implementing a marker strategy for the QoS policy, see [“How to Plan Forwarding Behavior” on page 708](#).

Flow Accounting (`flowacct`) Overview

IPQoS adds the `flowacct` accounting module to the Diffserv model. You can use `flowacct` to gather statistics on traffic flows, and bill customers in agreement with their SLAs. Flow accounting is also useful for capacity planning and system monitoring.

The `flowacct` module works with the `acctadm` command to create an accounting log file. A basic log includes the IPQoS 5-tuple and two additional attributes, as shown in the following list:

- Source address
- Source port
- Destination address
- Destination port
- Protocol number

- Number of packets
- Number of bytes

You can also gather statistics on other attributes, as described in “Recording Information About Traffic Flows” on page 752, and in the `flowacct(7ipp)` and `acctadm(1M)` man pages.

For information on planning a flow-accounting strategy, see “How to Plan for Flow Accounting” on page 710.

How Traffic Flows Through the IPQoS Modules

The next figure shows a path that incoming traffic might take through some of the IPQoS modules.

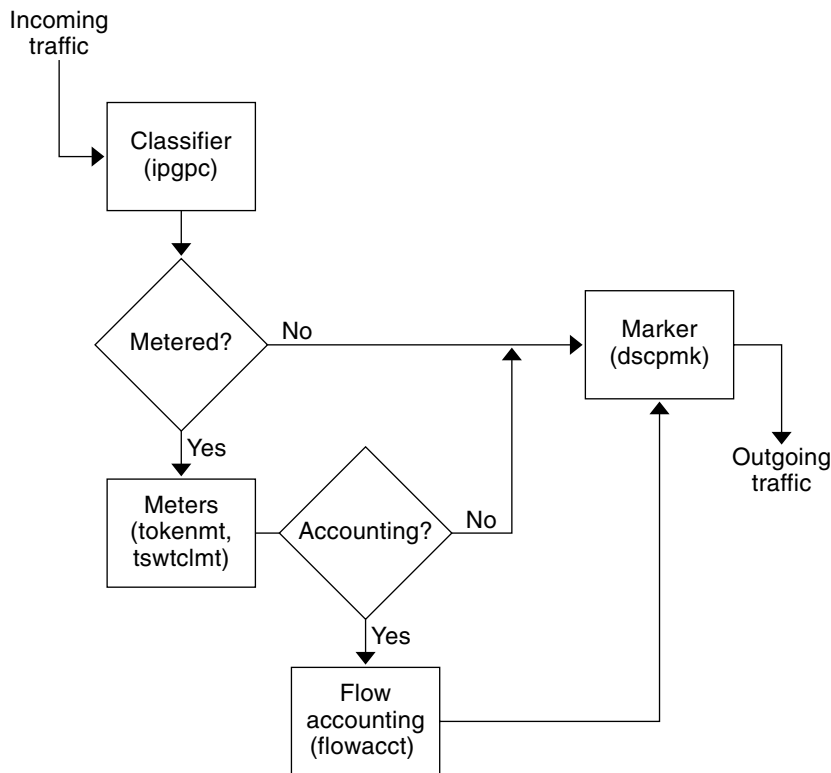


FIGURE 31-1 Traffic Flow Through the IPQoS Implementation of the Diffserv Model

This figure illustrates a common traffic flow sequence on an IPQoS-enabled machine:

1. The classifier selects from the packet stream all packets that match the filtering criteria in the system’s QoS policy.

2. The selected packets are then evaluated for the next action to be taken.
3. The classifier sends to the marker any traffic that does not require flow control.
4. Traffic to be flow-controlled is sent to the meter.
5. The meter enforces the configured rate. Then, the meter assigns a traffic conformance value to the flow-controlled packets.
6. The flow-controlled packets are then evaluated to determine if any packets require accounting.
7. The meter sends to the marker any traffic that does not require flow accounting.
8. The flow-accounting module gathers statistics on received packets. The module then sends the packets to the marker.
9. The marker assigns a DS codepoint to the packet header. This DSCP indicates the per-hop behavior that a Diffserv-aware system must apply to the packet.

Traffic Forwarding on an IPQoS-Enabled Network

This section introduces the elements that are involved in forwarding packets on an IPQoS-enabled network. An IPQoS-enabled system handles any packets on the network stream with the system's IP address as the destination. The IPQoS system then applies its QoS policy to the packet to establish differentiated services.

DS Codepoint

The DS codepoint (DSCP) defines in the packet header the action that any Diffserv-aware system should take on a marked packet. The diffserv architecture defines a set of DS codepoints for the IPQoS-enabled system and diffserv router to use. The Diffserv architecture also defines a set of actions that are called *forwarding behaviors*, which correspond to the DSCPs. The IPQoS-enabled system marks the precedence bits of the DS field in the packet header with the DSCP. When a router receives a packet with a DSCP value, the router applies the forwarding behavior that is associated with that DSCP. The packet is then released onto the network.

Note – The `d1cosmk` marker does not use the DSCP. Rather, `d1cosmk` marks Ethernet frame headers with a CoS value. If you plan to configure IPQoS on a network that uses VLAN devices, refer to [“Marker Module” on page 763](#).

Per-Hop Behaviors

In Diffserv terminology, the forwarding behavior that is assigned to a DSCP is called the *per-hop behavior (PHB)*. The PHB defines the forwarding precedence that a marked packet receives in relation to other traffic on the Diffserv-aware system. This precedence ultimately determines whether the IPQoS-enabled system or Diffserv router forwards or drops the marked packet. For a forwarded packet, each Diffserv router that the packet encounters en route to its destination applies the same PHB. The exception is if another Diffserv system changes the DSCP. For more information on PHBs, refer to “Using the `dscpmk` Marker for Forwarding Packets” on page 763.

The goal of a PHB is to provide a specified amount of network resources to a class of traffic on the contiguous network. You can achieve this goal in the QoS policy. Define DSCPs that indicate the precedence levels for traffic classes when the traffic flows leave the IPQoS-enabled system. Precedences can range from high-precedence/low-drop probability to low-precedence/high-drop probability.

For example, your QoS policy can assign to one class of traffic a DSCP that guarantees a low-drop PHB. This traffic class then receives a low-drop precedence PHB from any Diffserv-aware router, which guarantees bandwidth to packets of this class. You can add to the QoS policy other DSCPs that assign varying levels of precedence to other traffic classes. The lower-precedence packets are given bandwidth by Diffserv systems in agreement with the priorities that are indicated in the packets’ DSCPs.

IPQoS supports two types of forwarding behaviors, which are defined in the Diffserv architecture, expedited forwarding and assured forwarding.

Expedited Forwarding

The *expedited forwarding (EF)* per-hop behavior assures that any traffic class with EFs related DSCP is given highest priority. Traffic with an EF DSCP is not queued. EF provides low loss, latency, and jitter. The recommended DSCP for EF is 101110. A packet that is marked with 101110 receives guaranteed low-drop precedence as the packet traverses Diffserv-aware networks en route to its destination. Use the EF DSCP when assigning priority to customers or applications with a premium SLA.

Assured Forwarding

The *assured forwarding (AF)* per-hop behavior provides four different forwarding classes that you can assign to a packet. Every forwarding class provides three drop precedences, as shown in [Table 36-2](#).

The various AF codepoints provide the ability to assign different levels of service to customers and applications. In the QoS policy, you can prioritize traffic and services on your network when you plan the QoS policy. You can then assign different AF levels to the prioritized traffic.

Packet Forwarding in a Diffserv Environment

The following figure shows part of an intranet at a company with a partially Diffserv-enabled environment. In this scenario, all hosts on networks 10.10.0.0 and 10.14.0.0 are IPQoS enabled, and the local routers on both networks are Diffserv aware. However, the interim networks are not configured for Diffserv.

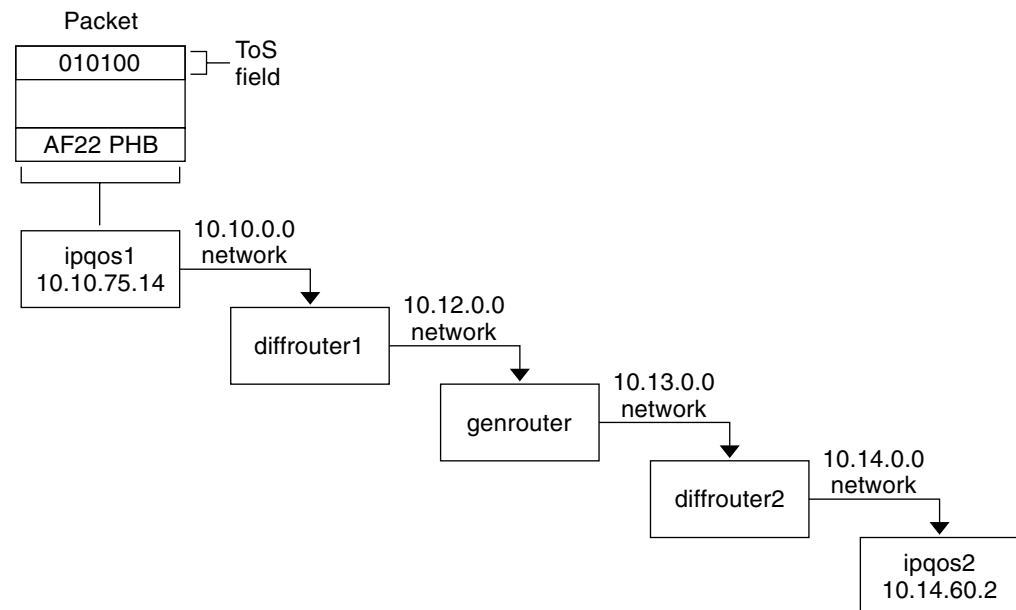


FIGURE 31-2 Packet Forwarding Across Diffserv-Aware Network Hops

The next steps trace the flow of the packet that is shown in this figure. The steps begin with the progress of a packet that originates at host ipqos1. The steps then continue through several hops to host ipqos2.

1. The user on ipqos1 runs the ftp command to access host ipqos2, which is three hops away.
2. ipqos1 applies its QoS policy to the resulting packet flow. ipqos1 then successfully classifies the ftp traffic.

The system administrator has created a class for all outgoing ftp traffic that originates on the local network 10.10.0.0. Traffic for the ftp class is assigned the AF22 per-hop behavior: class two, medium-drop precedence. A traffic flow rate of 2Mb/sec is configured for the ftp class.

3. ipqos-1 meters the ftp flow to determine if the flow exceeds the committed rate of 2 Mbit/sec.
4. The marker on ipqos1 marks the DS fields in the outgoing ftp packets with the 010100 DSCP, corresponding to the AF22 PHB.

5. The router `diffrouter1` receives the `ftp` packets. `diffrouter1` then checks the DSCP. If `diffrouter1` is congested, packets that are marked with AF22 are dropped.
6. `ftp` traffic is forwarded to the next hop in agreement with the per-hop behavior that is configured for AF22 in `diffrouter1`'s files.
7. The `ftp` traffic traverses network `10.12.0.0` to `genrouter`, which is not Diffserv aware. As a result, the traffic receives "best-effort" forwarding behavior.
8. `genrouter` passes the `ftp` traffic to network `10.13.0.0`, where the traffic is received by `diffrouter2`.
9. `diffrouter2` is Diffserv aware. Therefore, the router forwards the `ftp` packets to the network in agreement with the PHB that is defined in the router policy for AF22 packets.
10. `ipqos2` receives the `ftp` traffic. `ipqos2` then prompts the user on `ipqos1` for a user name and password.

Planning for an IPQoS-Enabled Network (Tasks)

You can configure IPQoS on any system that runs the Solaris OS. The IPQoS system then works with Diffserv-aware routers to provide differentiated services and traffic management on an intranet.

This chapter contains planning tasks for adding IPQoS-enabled systems onto a Diffserv-aware network. The following topics are covered.

- [“General IPQoS Configuration Planning \(Task Map\)” on page 695](#)
- [“Planning the Diffserv Network Topology” on page 696](#)
- [“Planning the Quality-of-Service Policy” on page 699](#)
- [“General IPQoS Configuration Planning \(Task Map\)” on page 695](#)
- [“Introducing the IPQoS Configuration Example” on page 711](#)

General IPQoS Configuration Planning (Task Map)

Implementing differentiated services, including IPQoS, on a network requires extensive planning. You must consider not only the position and function of each IPQoS-enabled system, but also each system’s relationship to the router on the local network. The following task map lists the major planning tasks for implementing IPQoS on your network.

Task	Description	For Instructions
1. Plan a Diffserv network topology that incorporates IPQoS-enabled systems.	Learn about the various Diffserv network topologies to determine the best solution for your site.	"Planning the Diffserv Network Topology" on page 696.
2. Plan the different types of services to be offered by the IPQoS systems.	Organize the types of services that the network provides into service-level agreements (SLAs).	"Planning the Quality-of-Service Policy" on page 699.
3. Plan the QoS policy for each IPQoS system.	Decide on the classes, metering, and accounting features that are needed to implement each SLA.	"Planning the Quality-of-Service Policy" on page 699.
4. If applicable, plan the policy for the Diffserv router.	Decide any scheduling and queuing policies for the Diffserv router that is used with the IPQoS systems.	Refer to router documentation for queuing and scheduling policies.

Planning the Diffserv Network Topology

To provide differentiated services for your network, you need at least one IPQoS-enabled system and a Diffserv-aware router. You can expand this basic scenario in a variety of ways, as explained in this section.

Hardware Strategies for the Diffserv Network

Typically, customers run IPQoS on servers and server consolidations, such as the Sun Enterprise™ 10000 server. Conversely, you can also run IPQoS on desktop systems such as UltraSPARC® systems, depending on the needs of your network. The following list describes possible systems for an IPQoS configuration:

- Solaris systems that offer various services, such as web servers and database servers
- Application servers that offer email, FTP, or other popular network applications
- Web cache servers or proxy servers
- Network of IPQoS-enabled server farms that are managed by Diffserv-aware load balancers
- Firewalls that manage traffic for a single heterogeneous network
- IPQoS systems that are part of a virtual local area network (LAN)

You might introduce IPQoS systems into a network topology with already functioning Diffserv-aware routers. If your router does not currently offer Diffserv, consider the Diffserv solutions that are offered by Cisco Systems, Juniper Networks, and other router manufacturers. If the local router does not implement Diffserv, then the router passes marked packets on to the next hop without evaluating the marks.

IPQoS Network Topologies

This section illustrates IPQoS strategies for various network needs.

IPQoS on Individual Hosts

The following figure shows a single network of IPQoS-enabled systems.

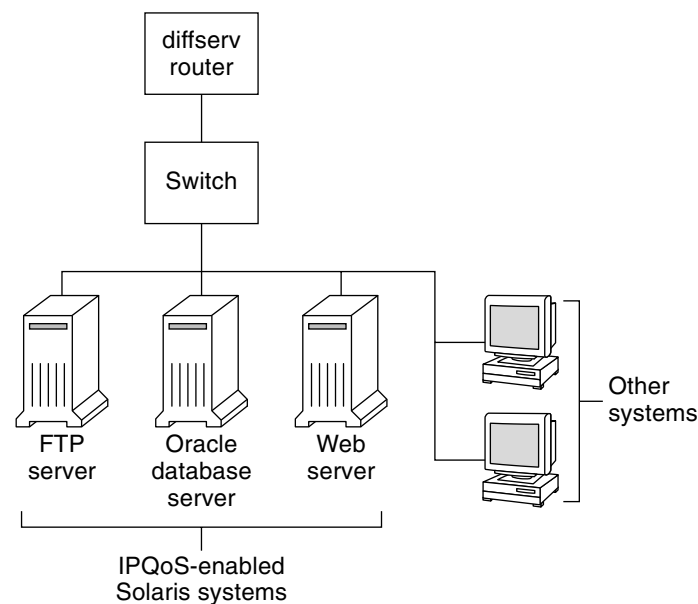


FIGURE 32-1 IPQoS Systems on a Network Segment

This network is but one segment of a corporate intranet. By enabling IPQoS on the application servers and web servers, you can control the rate at which each IPQoS system releases outgoing traffic. If you make the router Diffserv aware, you can further control incoming and outgoing traffic.

The examples in this guide use the “IPQoS on an individual host” scenario. For the example topology that is used throughout the guide, see [Figure 32-4](#).

IPQoS on a Network of Server Farms

The following figure shows a network with several heterogeneous server farms.

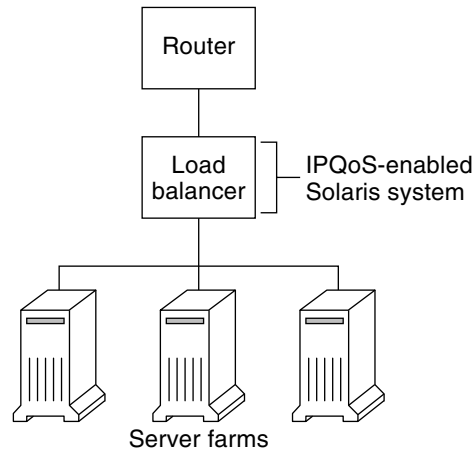


FIGURE 32-2 Network of IPQoS-Enabled Server Farms

In such a topology, the router is Diffserv aware, and therefore able to queue and rate both incoming and outgoing traffic. The load balancer is also Diffserv-aware, and the server farms are IPQoS enabled. The load balancer can provide additional filtering beyond the router by using selectors such as user ID and project ID. These selectors are included in the application data.

This scenario provides flow control and traffic forwarding to manage congestion on the local network. This scenario also prevents outgoing traffic from the server farms from overloading other portions of the intranet.

IPQoS on a Firewall

The following figure shows a segment of a corporate network that is secured from other segments by a firewall.

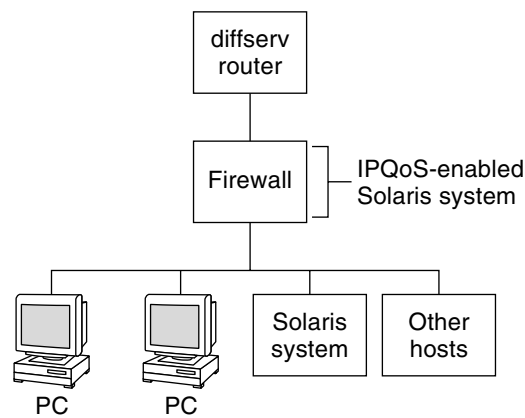


FIGURE 32-3 Network Protected by an IPQoS-Enabled Firewall

In this scenario, traffic flows into a Diffserv-aware router where the packets are filtered and queued. All incoming traffic that is forwarded by the router then travels into the IPQoS-enabled firewall. To use IPQoS, the firewall must not bypass the IP forwarding stack.

The firewall's security policy determines whether incoming traffic is permitted to enter or depart the internal network. The QoS policy controls the service levels for incoming traffic that has passed the firewall. Depending on the QoS policy, outgoing traffic can also be marked with a forwarding behavior.

Planning the Quality-of-Service Policy

When you plan the quality-of-service (QoS) policy, you must review, classify, and then prioritize the services that your network provides. You must also assess the amount of available bandwidth to determine the rate at which each traffic class is released onto the network.

QoS Policy Planning Aids

Gather information for planning the QoS policy in a format that includes the information needed for the IPQoS configuration file. For example, you can use the following template to list the major categories of information to be used in the IPQoS configuration file.

TABLE 32-1 QoS Planning Template

Class	Priority	Filter	Selector	Rate	Forwarding?	Accounting?
Class 1	1	Filter 1	Selector 1	Meter rates, depending on meter type	Marker drop precedence	Requires flow-accounting statistics
		Filter 3	Selector 2			
Class 1	1	Filter 2	Selector 1	N/A	N/A	N/A
			Selector 2			
Class 2	2	Filter 1	Selector 1	Meter rates, depending on meter type	Marker drop precedence	Requires flow-accounting statistics
			Selector 2			
Class 2	2	Filter 2	Selector 1	N/A	N/A	N/A
			Selector 2			

You can divide each major category to further define the QoS policy. Subsequent sections explain how to obtain information for the categories that are shown in the template.

QoS Policy Planning (Task Map)

This task map lists the major tasks for planning a QoS policy.

Task	Description	For Instructions
1. Design your network topology to support IPQoS.	Identify the hosts and routers on your network to provide differentiated services.	“How to Prepare a Network for IPQoS” on page 701
2. Define the classes into which services on your network must be divided.	Examine the types of services and SLAs that are offered by your site, and determine the discrete traffic classes into which these services fall.	“How to Define the Classes for Your QoS Policy” on page 702
3. Define filters for the classes.	Determine the best ways of separating traffic of a particular class from the network traffic flow.	“How to Define Filters in the QoS Policy” on page 705
4. Define flow-control rates for measuring traffic as packets leave the IPQoS system.	Determine acceptable flow rates for each class of traffic.	“How to Plan Flow Control” on page 706

Task	Description	For Instructions
5. Define DSCPs or user-priority values to be used in the QoS policy.	Plan a scheme to determine the forwarding behavior that is assigned to a traffic flow when the flow is handled by the router or switch.	“How to Plan Forwarding Behavior” on page 708
6. If applicable, set up a statistics-monitoring plan for traffic flows on the network.	Evaluate the traffic classes to determine which traffic flows must be monitored for accounting or statistical purposes.	“How to Plan for Flow Accounting” on page 710

Note – The rest of this section explains how to plan the QoS policy of an IPQoS-enabled system. To plan the QoS policy for the Diffserv router, refer to the router documentation and the router manufacturer’s web site.

▼ How to Prepare a Network for IPQoS

The following procedure lists general planning tasks to do before you create the QoS policy.

- Steps**
- 1. Review your network topology. Then, plan a strategy that uses IPQoS systems and Diffserv routers.**
For topology examples, see [“Planning the Diffserv Network Topology” on page 696](#).
 - 2. Identify the hosts in the topology that require IPQoS or that might become good candidates for IPQoS service.**
 - 3. Determine which IPQoS-enabled systems could use the same QoS policy.**
For example, if you plan to enable IPQoS on all hosts on the network, identify any hosts that could use the same QoS policy. Each IPQoS-enabled system must have a local QoS policy, which is implemented in its IPQoS configuration file. However, you can create one IPQoS configuration file to be used by a range of systems. You can then copy the configuration file to every system with the same QoS policy requirements.
 - 4. Review and perform any planning tasks that are required by the Diffserv router on your network.**
Refer to the router documentation and the router manufacturer’s web site for details.

▼ How to Define the Classes for Your QoS Policy

The first step in defining the QoS policy is organizing traffic flows into classes. You do not need to create classes for every type of traffic on a Diffserv network. Moreover, depending on your network topology, you might have to create a different QoS policy for each IPQoS-enabled system.

Note – For an overview of classes, see [“Classes” on page 687](#).

The next procedure assumes that you have determined which systems on your network are to be IPQoS-enabled, as identified in [“How to Prepare a Network for IPQoS” on page 701](#).

Steps 1. **Create a QoS planning table for organizing the QoS policy information.**

For suggestions, refer to [Table 32–1](#).

2. **Perform the remaining steps for every QoS policy that is on your network.**

3. **Define the classes to be used in the QoS policy.**

The following questions are a guideline for analyzing network traffic for possible class definitions.

■ **Does your company offer service-level agreements to customers?**

If yes, then evaluate the relative priority levels of the SLAs that your company offers to customers. The same applications might be offered to customers who are guaranteed different priority levels.

For example, your company might offer web site hosting to each customer, which indicates that you need to define a class for each customer web site. One SLA might provide a premium web site as one service level. Another SLA might offer a “best-effort” personal web site to discount customers. This factor indicates not only different web site classes but also potentially different per-hop behaviors that are assigned to the web site classes.

■ **Does the IPQoS system offer popular applications that might need flow control?**

You can improve network performance by enabling IPQoS on servers offering popular applications that generate excessive traffic. Common examples are electronic mail, network news, and FTP. Consider creating separate classes for incoming and outgoing traffic for each service type, where applicable. For example, you might create a mail-in class and a mail-out class for the QoS policy for a mail server.

■ **Does your network run certain applications that require highest-priority forwarding behaviors?**

Any critical applications that require highest-priority forwarding behaviors must receive highest priority in the router's queue. Typical examples are streaming video and streaming audio.

Define incoming classes and outgoing classes for these high-priority applications. Then, add the classes to the QoS policies of both the IPQoS-enabled system that serves the applications and the Diffserv router.

- **Does your network experience traffic flows that must be controlled because the flows consume large amounts of bandwidth?**

Use `netstat`, `snoop`, and other network monitoring utilities to discover the types of traffic that are causing problems on the network. Review the classes that you have created thus far, and then create new classes for any undefined problem traffic category. If you have already defined classes for a category of problem traffic, then define rates for the meter to control the problem traffic.

Create classes for the problem traffic on every IPQoS-enabled system on the network. Each IPQoS system can then handle any problem traffic by limiting the rate at which the traffic flow is released onto the network. Be sure also to define these problem classes in the QoS policy on the Diffserv router. The router can then queue and schedule the problem flows as configured in its QoS policy.

- **Do you need to obtain statistics on certain types of traffic?**

A quick review of an SLA can indicate which types of customer traffic require accounting. If your site does offer SLAs, you probably have already created classes for traffic that requires accounting. You might also define classes to enable statistics gathering on traffic flows that you are monitoring. You could also create classes for traffic to which you restrict access for security reasons.

4. **List the classes that you have defined in the QoS planning table you created in Step 1.**

5. **Assign a priority level to each class.**

For example, have priority level 1 represent the highest-priority class, and assign descending-level priorities to the remaining classes. The priority level that you assign is for organizational purposes only. Priority levels that you set in the QoS policy template are not actually used by IPQoS. Moreover, you can assign the same priority to more than one class, if appropriate for your QoS policy.

6. **When you finish defining classes, you next define filters for each class, as explained in [“How to Define Filters in the QoS Policy”](#) on page 705.**

More Information

Prioritizing the Classes

As you create classes, you quickly realize which classes have highest priority, medium priority, and best-effort priority. A good scheme for prioritizing classes becomes particularly important when you assign per-hop behaviors to outgoing traffic, as explained in [“How to Plan Forwarding Behavior”](#) on page 708.

In addition to assigning a PHB to a class, you can also define a priority selector in a filter for the class. The priority selector is active on the IPQoS-enabled host only. Suppose several classes with equal rates and identical DSCPs sometimes compete for bandwidth as they leave the IPQoS system. The priority selector in each class can further order the level of service that is given to the otherwise identically valued classes.

Defining Filters

You create filters to identify packet flows as members of a particular class. Each filter contains selectors, which define the criteria for evaluating a packet flow. The IPQoS-enabled system then uses the criteria in the selectors to extract packets from a traffic flow. The IPQoS system then associates the packets with a class. For an introduction to filters, see [“Filters” on page 688](#).

The following table lists the most commonly used selectors. The first five selectors represent the IPQoS 5-tuple, which the IPQoS system uses to identify packets as members of a flow. For a complete list of selectors, see [Table 36–1](#).

TABLE 32–2 Common IPQoS Selectors

Name	Definition
saddr	Source address.
daddr	Destination address.
sport	Source port number. You can use a well-known port number, as defined in <code>/etc/services</code> , or a user-defined port number.
dport	Destination port number.
protocol	IP protocol number or protocol name that is assigned to the traffic flow type in <code>/etc/protocols</code> .
ip_version	Addressing style to use. Use either IPv4 or IPv6. IPv4 is the default.
dsfield	Contents of the DS field, that is, the DSCP. Use this selector for extracting incoming packets that are already marked with a particular DSCP.
priority	Priority level that is assigned to the class. For more information, see “How to Define the Classes for Your QoS Policy” on page 702 .
user	Either the UNIX user ID or user name that is used when the upper-level application is executed.
projid	Project ID that is used when the upper-level application is executed.
direction	Direction of traffic flow. Value is either <code>LOCAL_IN</code> , <code>LOCAL_OUT</code> , <code>FWD_IN</code> , or <code>FWD_OUT</code> .

Note – Be judicious in your choice of selectors. Use only as many selectors as you need to extract packets for a class. The more selectors that you define, the greater the impact on IPQoS performance.

▼ How to Define Filters in the QoS Policy

Before You Begin Before you can perform the next steps, you should have completed the procedure “How to Define the Classes for Your QoS Policy” on page 702.

- Steps**
1. **Create at least one filter for each class in the QoS planning table that you created in “How to Define the Classes for Your QoS Policy” on page 702.**
Consider creating separate filters for incoming and outgoing traffic for each class, where applicable. For example, add an `ftp-in` filter and an `ftp-out` filter to the QoS policy of an IPQoS-enabled FTP server. You then can define an appropriate `direction` selector in addition to the basic selectors.
 2. **Define at least one selector for each filter in a class.**
Use the QoS planning table that was introduced in Table 32–1 to fill in filters for the classes you defined.

Example 32–1 Defining Filters for FTP Traffic

The next table shows how you would define a filter for outgoing FTP traffic.

Class	Priority	Filters	Selectors
ftp-traffic	4	ftp-out	saddr 10.190.17.44 daddr 10.100.10.53 sport 21 direction LOCAL_OUT

- See Also**
- To define a flow-control scheme, refer to “How to Plan Flow Control” on page 706.
 - To define forwarding behaviors for flows as the flows return to the network stream, refer to “How to Plan Forwarding Behavior” on page 708.
 - To plan for flow accounting of certain types of traffic, refer to “How to Plan for Flow Accounting” on page 710.
 - To add more classes to the QoS policy, refer to “How to Define the Classes for Your QoS Policy” on page 702.
 - To add more filters to the QoS policy, refer to “How to Define Filters in the QoS Policy” on page 705.

▼ How to Plan Flow Control

Flow control involves measuring traffic flow for a class and then releasing packets onto the network at a defined rate. When you plan flow control, you define parameters to be used by the IPQoS metering modules. The meters determine the rate at which traffic is released onto the network. For an introduction to the metering modules, see [“Meter \(tokenmt and tswtclmt\) Overview” on page 688](#).

The next procedure assumes that you have defined filters and selectors, as described in [“How to Define Filters in the QoS Policy” on page 705](#).

- Steps**
1. **Determine the maximum bandwidth for your network.**
 2. **Review any SLAs that are supported on your network. Identify customers and the type of service that is guaranteed to each customer.**

To guarantee a certain level of service, you might need to meter certain traffic classes that are generated by the customer.

3. **Review the list of classes that you created in [“How to Define the Classes for Your QoS Policy” on page 702](#).**

Determine if any classes other than those classes that are associated with SLAs need to be metered.

Suppose the IPQoS system runs an application that generates a high level of traffic. After you classify the application’s traffic, meter the flows to control the rate at which the packets of the flow return to the network.

Note – Not all classes need to be metered. Remember this guideline as you review your list of classes.

4. **Determine which filters in each class select traffic that needs flow control. Then, refine your list of classes that require metering.**

Classes that have more than one filter might require metering for only one filter. Suppose that you define filters for incoming and outgoing traffic of a certain class. You might conclude that only traffic in one direction requires flow control.

5. **Choose a meter module for each class to be flow controlled.**

Add the module name to the meter column in your QoS planning table.

6. **Add the rates for each class to be metered to the organizational table.**

If you use the `tokenmt` module, you need to define the following rates in bits per second:

- Committed rate
- Peak rate

If these rates are sufficient to meter a particular class, you can define only the committed rate and the committed burst for `tokenmt`.

If needed, you can also define the following rates:

- Committed burst
- Peak burst

For a complete definition of `tokenmt` rates, refer to [“Configuring `tokenmt` as a Two-Rate Meter” on page 761](#). You can also find more detailed information in the `tokenmt(7ipp)` man page.

If you use the `tswtclmt` module, you need to define the following rates in bits per second.

- Committed rate
- Peak rate

You can also define the window size in milliseconds. These rates are defined in [“`tswtclmt` Metering Module” on page 762](#) and in the `twstclmt(7ipp)` man page.

7. Add traffic conformance outcomes for the metered traffic.

The outcomes for both metering modules are green, red, and yellow. Add to your QoS organizational table the traffic conformance outcomes that apply to the rates you define. Outcomes for the meters are fully explained in [“Meter Module” on page 760](#).

You need to determine what action should be taken on traffic that conforms, or does not conform, to the committed rate. Often, but not always, this action is to mark the packet header with a per-hop behavior. One acceptable action for green-level traffic could be to continue processing while traffic flows do not exceed the committed rate. Another action could be to drop packets of the class if flows exceed peak rate.

Example 32–2 Defining Meters

The next table shows meter entries for a class of email traffic. The network on which the IPQoS system is located has a total bandwidth of 100 Mbits/sec, or 10000000 bits per second. The QoS policy assigns a low priority to the email class. This class also receives best-effort forwarding behavior.

Class	Priority	Filter	Selector	Rate
email	8	mail_in	daddr10.50.50.5 dport imap direction LOCAL_IN	

Class	Priority	Filter	Selector	Rate
email	8	mail_out	saddr10.50.50.5	meter=tokenmt
			sport imap	committed rate=5000000
			direction LOCAL_OUT	committed burst =5000000 peak rate =10000000 peak burst=1000000 green precedence=continue processing yellow precedence=mark yellow PHB red precedence=drop

- See Also**
- To define forwarding behaviors for flows as the packets return to the network stream, refer to [“How to Plan Forwarding Behavior”](#) on page 708.
 - To plan for flow accounting of certain types of traffic, refer to [“How to Plan for Flow Accounting”](#) on page 710.
 - To add more classes to the QoS policy, refer to [“How to Define the Classes for Your QoS Policy”](#) on page 702.
 - To add more filters to the QoS policy, refer to [“How to Define Filters in the QoS Policy”](#) on page 705.
 - To define another flow-control scheme, refer to [“How to Plan Flow Control”](#) on page 706.
 - To create an IPQoS configuration file, refer to [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

▼ How to Plan Forwarding Behavior

Forwarding behavior determines the priority and drop precedence of traffic flows that are about to be forwarded to the network. You can choose two major forwarding behaviors: prioritize the flows of a class in relationship to other traffic classes or drop the flows entirely.

The Diffserv model uses the marker to assign the chosen forwarding behavior to traffic flows. IPQoS offers the following marker modules.

- `dscpmk` – Used to mark the DS field of an IP packet with a DSCP
- `d1cosmk` – Used to mark the VLAN tag of a datagram with a class-of-service (CoS) value

Note – The suggestions in this section refer specifically to IP packets. If your IPQoS system includes a VLAN device, you can use the `d1cosmk` marker to mark forwarding behaviors for datagrams. For more information, refer to [“Using the d1cosmk Marker With VLAN Devices”](#) on page 765.

To prioritize IP traffic, you need to assign a DSCP to each packet. The `dscpmk` marker marks the DS field of the packet with the DSCP. You choose the DSCP for a class from a group of well-known codepoints that are associated with the forwarding behavior type. These well-known codepoints are 46 (101110) for the EF PHB and a range of codepoints for the AF PHB. For overview information on DSCP and forwarding, refer to [“Traffic Forwarding on an IPQoS-Enabled Network”](#) on page 691.

Before You Begin The next steps assume that you have defined classes and filters for the QoS policy. Though you often use the meter with the marker to control traffic, you can use the marker alone to define a forwarding behavior.

Steps 1. **Review the classes that you have created thus far and the priorities that you have assigned to each class.**

Not all traffic classes need to be marked.

2. **Assign the EF per-hop behavior to the class with the highest priority.**

The EF PHB guarantees that packets with the EF DSCP 46 (101110) are released onto the network before packets with any AF PHBs. Use the EF PHB for your highest-priority traffic. For more information about EF, refer to [“Expedited Forwarding \(EF\) PHB”](#) on page 764.

3. **Assign forwarding behaviors to classes that have traffic to be metered.**

4. **Assign DS codepoints to the remaining classes in agreement with the priorities that you have assigned to the classes.**

Example 32–3 QoS Policy for a Games Application

Traffic is generally metered for the following reasons:

- An SLA guarantees packets of this class greater service or lesser service when the network is heavily used.
- A class with a lower priority might have a tendency to flood the network.

You use the marker with the meter to provide differentiated services and bandwidth management to these classes. For example, the following table shows a portion of a QoS policy. This policy defines a class for a popular games application that generates a high level of traffic.

Class	Priority	Filter	Selector	Rate	Forwarding?
games_app	9	games_in	sport 6080	N/A	N/A
games_app	9	games_out	dport 6081	meter=tokenmt committed rate=5000000 committed burst =5000000 peak rate =10000000 peak burst=15000000 green precedence=continue processing yellow precedence=mark yellow PHB red precedence=drop	green =AF31 yellow=AF42 red=drop

The forwarding behaviors assign low-priority DSCPs to `games_app` traffic that conforms to its committed rate or is under the peak rate. When `games_app` traffic exceeds peak rate, the QoS policy indicates that packets from `games_app` are to be dropped. All AF codepoints are listed in [Table 36-2](#).

- See Also**
- To plan for flow accounting of certain types of traffic, refer to [“How to Plan for Flow Accounting”](#) on page 710.
 - To add more classes to the QoS policy, refer to [“How to Define the Classes for Your QoS Policy”](#) on page 702.
 - To add more filters to the QoS policy, refer to [“How to Define Filters in the QoS Policy”](#) on page 705.
 - To define a flow-control scheme, refer to [“How to Plan Flow Control”](#) on page 706.
 - To define additional forwarding behaviors for flows as the packets return to the network stream, refer to [“How to Plan Forwarding Behavior”](#) on page 708.
 - To create an IPQoS configuration file, refer to [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

▼ How to Plan for Flow Accounting

You use the IPQoS `flowacct` module to track traffic flows for billing or network management purposes. Use the following procedure to determine if your QoS policy should include flow accounting.

Steps 1. **Does your company offer SLAs to customers?**

If the answer is yes, then you should use flow accounting. Review the SLAs to determine what types of network traffic your company wants to bill customers for. Then, review your QoS policy to determine which classes select traffic to be billed.

2. **Are there applications that might need monitoring or testing to avoid network problems?**

If the answer is yes, consider using flow accounting to observe the behavior of these applications. Review your QoS policy to determine the classes that you have assigned to traffic that requires monitoring.

3. **Mark Y in the flow-accounting column for each class that requires flow accounting in your QoS planning table.**

- See Also**
- To add more classes to the QoS policy, refer to [“How to Define the Classes for Your QoS Policy”](#) on page 702.
 - To add more filters to the QoS policy, refer to [“How to Define Filters in the QoS Policy”](#) on page 705.
 - To define a flow-control scheme, refer to [“How to Plan Flow Control”](#) on page 706.
 - To define forwarding behaviors for flows as the packets return to the network stream, refer to [“How to Plan Forwarding Behavior”](#) on page 708.
 - To plan for additional flow accounting of certain types of traffic, refer to [“How to Plan for Flow Accounting”](#) on page 710.
 - To create the IPQoS configuration file, refer to [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

Introducing the IPQoS Configuration Example

Tasks in the remaining chapters of the guide use the example IPQoS configuration that is introduced in this section. The example shows the differentiated services solution on the public intranet of BigISP, a fictitious service provider. BigISP offers services to large companies that reach BigISP through leased lines. Individuals who dial in from modems can also buy services from BigISP.

IPQoS Topology

The following figure shows the network topology that is used for BigISP’s public intranet.

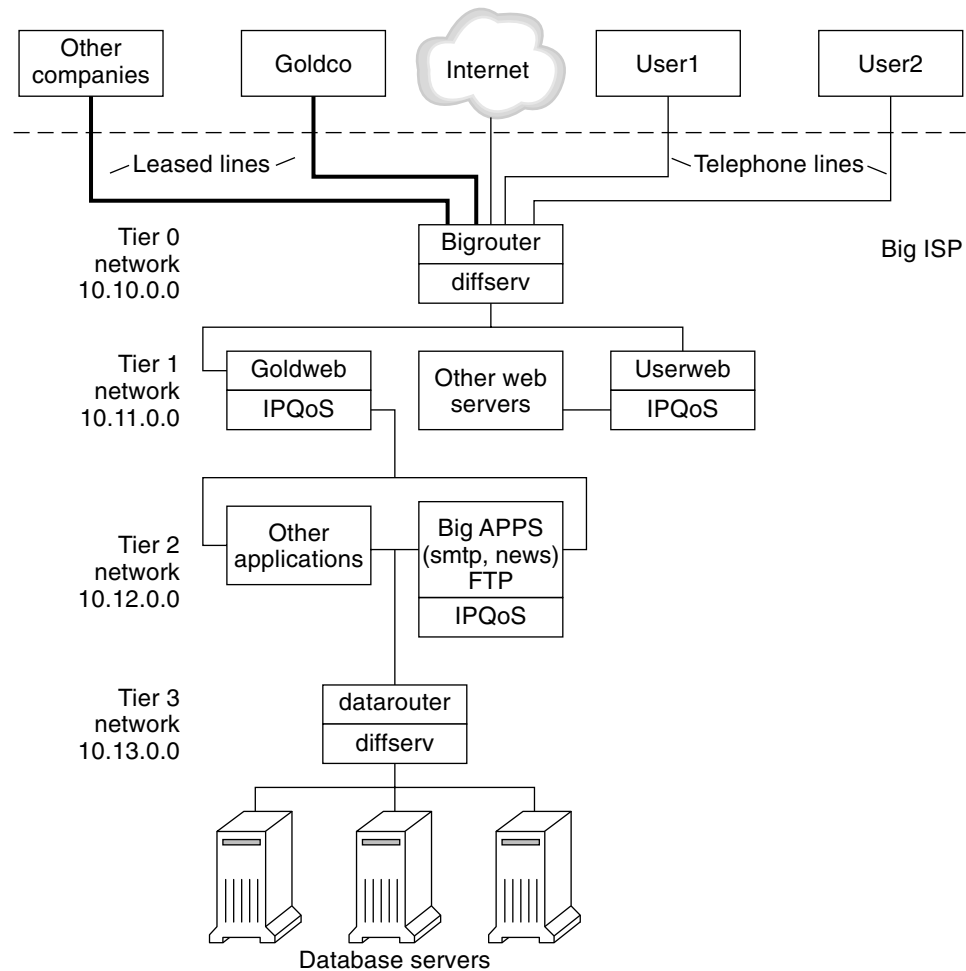


FIGURE 32-4 IPQoS Example Topology

BigISP has implemented these four tiers in its public intranet:

- **Tier 0** – Network 10.10.0.0 includes a large Diffserv router that is called *Bigrouter*, which has both external and internal interfaces. Several companies, including a large organization that is called *Goldco*, have rented leased-line services that terminate at *Bigrouter*. Tier 0 also handles individual customers who call over telephone lines or ISDN.
- **Tier 1** – Network 10.11.0.0 provides web services. The *Goldweb* server hosts the web site which was purchased by *Goldco* as part of the premium service that *Goldco* has purchased from *BigISP*. The server *Userweb* hosts small web sites that were purchased by individual customers. Both *Goldweb* and *Userweb* are IPQoS

enabled.

- **Tier 2** – Network 10.12.0.0 provides applications for all customers to use. BigAPPS, one of the application servers, is IPQoS-enabled. BigAPPS provides SMTP, News, and FTP services.
- **Tier 3** – Network 10.13.0.0 houses large database servers. Access to Tier 3 is controlled by datarouter, a Diffserv router.

Creating the IPQoS Configuration File (Tasks)

This chapter shows how to create IPQoS configuration files. Topics that are covered in the chapter include the following.

- [“Defining a QoS Policy in the IPQoS Configuration File \(Task Map\)”](#) on page 715
- [“Tools for Creating a QoS Policy”](#) on page 717
- [“Creating IPQoS Configuration Files for Web Servers”](#) on page 718
- [“Creating an IPQoS Configuration File for an Application Server”](#) on page 731
- [“Providing Differentiated Services on a Router”](#) on page 741

This chapter assumes that you have defined a complete QoS policy, and you are ready to use this policy as the basis for the IPQoS configuration file. For instructions on QoS policy planning, refer to [“Planning the Quality-of-Service Policy”](#) on page 699.

Defining a QoS Policy in the IPQoS Configuration File (Task Map)

This task map lists the general tasks for creating an IPQoS configuration file.

Task	Description	For Instructions
1. Plan your IPQoS-enabled network configuration.	Decide which systems on the local network should become IPQoS enabled.	“How to Prepare a Network for IPQoS” on page 701
2. Plan the QoS policy for IPQoS systems on your network.	Identify traffic flows as distinct classes of service. Then, determine which flows require traffic management.	“Planning the Quality-of-Service Policy” on page 699

Task	Description	For Instructions
3. Create the IPQoS configuration file and define its first action.	Create the IPQoS file, invoke the IP classifier, and define a class for processing.	"How to Create the IPQoS Configuration File and Define Traffic Classes" on page 720
4. Create filters for a class.	Add the filters that govern which traffic is selected and organized into a class.	"How to Define Filters in the IPQoS Configuration File" on page 722
5. Add more classes and filters to the IPQoS configuration file.	Create more classes and filters to be processed by the IP classifier.	"How to Create an IPQoS Configuration File for a Best-Effort Web Server" on page 728
6. Add an <code>action</code> statement with parameters that configure the metering modules.	If the QoS policy calls for flow control, assign flow-control rates and conformance levels to the meter.	"How to Configure Flow Control in the IPQoS Configuration File" on page 737
7. Add an <code>action</code> statement with parameters that configure the marker.	If the QoS policy calls for differentiated forwarding behaviors, define how traffic classes are to be forwarded.	"How to Define Traffic Forwarding in the IPQoS Configuration File" on page 724
8. Add an <code>action</code> statement with parameters that configure the flow-accounting module.	If the QoS policy calls for statistics gathering on traffic flows, define how accounting statistics are to be gathered.	"How to Enable Accounting for a Class in the IPQoS Configuration File" on page 727
9. Apply the IPQoS configuration file.	Add the content of a specified IPQoS configuration file into the appropriate kernel modules.	"How to Apply a New Configuration to the IPQoS Kernel Modules" on page 744
10. Configure forwarding behaviors in the router files.	If any IPQoS configuration files on the network define forwarding behaviors, add the resulting DSCPs to the appropriate scheduling files on the router.	"How to Configure a Router on an IPQoS-Enabled Network" on page 741

Tools for Creating a QoS Policy

The QoS policy for your network resides in the IPQoS configuration file. You create this configuration file with a text editor. Then, you provide the file as an argument to `ipqosconf`, the IPQoS configuration utility. When you instruct `ipqosconf` to apply the policy that is defined in your configuration file, the policy is written into the kernel IPQoS system. For detailed information about the `ipqosconf` command, refer to the `ipqosconf(1M)` man page. For instructions on the use of `ipqosconf`, refer to “How to Apply a New Configuration to the IPQoS Kernel Modules” on page 744.

Basic IPQoS Configuration File

An IPQoS configuration file consists of a tree of `action` statements that implement the QoS policy that you defined in “Planning the Quality-of-Service Policy” on page 699. The IPQoS configuration file configures the IPQoS modules. Each action statement contains a set of *classes*, *filters*, or *parameters* to be processed by the module that is called in the action statement.

For the complete syntax of the IPQoS configuration file, refer to [Example 36-3](#) and the `ipqosconf(1M)` man page.

Configuring the IPQoS Example Topology

The tasks in this chapter explain how to create IPQoS configuration files for three IPQoS-enabled systems. These systems are part of the network topology of the company BigISP, which was introduced in [Figure 32-4](#).

- **Goldweb** – A web server that hosts web sites for customers who have purchased premium-level SLAs
- **Userweb** – A less-powerful web server that hosts personal web sites for home users who have purchased “best-effort” SLAs
- **BigAPPS** – An application server that serves mail, network news, and FTP to both gold-level and best-effort customers

These three configuration files illustrate the most common IPQoS configurations. You might use the sample files that are shown in the next section as templates for your own IPQoS implementation.

Creating IPQoS Configuration Files for Web Servers

This section introduces the IPQoS configuration file by showing how to create a configuration for a premium web server. The section then shows how to configure a completely different level of service in another configuration file for a server that hosts personal web sites. Both servers are part of the network example that is shown in [Figure 32-4](#).

The following configuration file defines IPQoS activities for the Goldweb server. This server hosts the web site for Goldco, the company that has purchased a premium SLA.

EXAMPLE 33-1 Sample IPQoS Configuration File for a Premium Web Server

```
fmt_version 1.0

action {
  module ipgpc
  name ipgpc.classify
  params {
    global_stats TRUE
  }
  class {
    name goldweb
    next_action markAF11
    enable_stats FALSE
  }
  class {
    name video
    next_action markEF
    enable_stats FALSE
  }
  filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
  }
  filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
  }
}

action {
  module dscpmk
  name markAF11
  params {
    global_stats FALSE
  }
}
```

EXAMPLE 33-1 Sample IPQoS Configuration File for a Premium Web Server (Continued)

```
        dscp_map{0-63:10}
        next_action continue
    }
}
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
action {
    module flowacct
    name acct
    params {
        enable_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
    }
}
```

The following configuration file defines IPQoS activities on Userweb. This server hosts web sites for individuals with low-priced, or *best-effort*, SLAs. This level of service guarantees the best service that can be delivered to best-effort customers after the IPQoS system handles traffic from customers with more expensive SLAs.

EXAMPLE 33-2 Sample Configuration for a Best-Effort Web Server

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name Userweb
        next_action markAF12
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class Userweb
    }
}
```

EXAMPLE 33-2 Sample Configuration for a Best-Effort Web Server (Continued)

```
action {
  module dscpmk
  name markAF12
  params {
    global_stats FALSE
    dscp_map{0-63:12}
    next_action continue
  }
}
```

▼ How to Create the IPQoS Configuration File and Define Traffic Classes

You can create your first IPQoS configuration file in whatever directory is easiest for you to maintain. The tasks in this chapter use the directory `/var/ipqos` as the location for IPQoS configuration files. The next procedure builds the initial segment of the IPQoS configuration file that is introduced in [Example 33-1](#).

Note – As you create the IPQoS configuration file, be very careful to start and end each `action` statement and clause with curly braces (`{ }`). For an example of the use of braces, see [Example 33-1](#).

Steps 1. **Log in to the premium web server, and create a new IPQoS configuration file with a `.qos` extension.**

Every IPQoS configuration file must start with the version number `fmt_version 1.0` as its first uncommented line.

2. **Follow the opening parameter with the initial action statement, which configures the generic IP classifier `ipgpc`.**

This initial action begins the tree of `action` statements that compose the IPQoS configuration file. For example, the `/var/ipqos/Goldweb.qos` file begins with the initial `action` statement to call the `ipgpc` classifier.

```
fmt_version 1.0
```

```
action {
  module ipgpc
  name ipgpc.classify
```

```
fmt_version 1.0
```

Begins the IPQoS configuration file.

```
action {
```

Begins the action statement.

```
module ipgpc
```

Configures the `ipgpc` classifier as the first action in the configuration file.

`name ipgpc.classify` Defines the name of the classifier action statement, which must always be `ipgpc.classify`.

For detailed syntactical information about action statements, refer to “[action Statement](#)” on page 771 and the `ipqosconf(1M)` man page.

3. Add a `params` clause with the statistics parameter `global_stats`.

```
params {
    global_stats TRUE
}
```

The parameter `global_stats TRUE` in the `ipgpc.classify` statement enables statistics gathering for that action. `global_stats TRUE` also enables per-class statistics gathering wherever a class clause definition specifies `enable_stats TRUE`.

Turning on statistics impacts performance. You might want to gather statistics on a new IPQoS configuration file to verify that IPQoS works properly. Later, you can turn off statistics collection by changing the argument to `global_stats` to `FALSE`.

Global statistics are but one type of parameter you can define in a `params` clause. For syntactical and other details about `params` clauses, refer to “[params Clause](#)” on page 773 and the `ipqosconf(1M)` man page.

4. Define a class that identifies traffic that is bound for the premium server.

```
class {
    name goldweb
    next_action markAF11
    enable_stats FALSE
}
```

This statement is called a *class clause*. A class clause has the following contents.

<code>name goldweb</code>	Creates the class <code>goldweb</code> to identify traffic that is bound for the Goldweb server.
<code>next_action markAF11</code>	Instructs the <code>ipgpc</code> module to pass packets of the <code>goldweb</code> class to the <code>markAF11</code> action statement. The <code>markAF11</code> action statement calls the <code>dscpnmk</code> marker.
<code>enable_stats FALSE</code>	Enables statistics taking for the <code>goldweb</code> class. However, because the value of <code>enable_stats</code> is <code>FALSE</code> , statistics for this class are not turned on.

For detailed information about the syntax of the class clause, see “[class Clause](#)” on page 772 and the `ipqosconf(1M)` man page.

5. Define a class that identifies an application that must have highest-priority forwarding.

```
class {
    name video
    next_action markEF
    enable_stats FALSE
}
```

<code>}</code>	
<code>name video</code>	Creates the class <code>video</code> to identify streaming video traffic that is outgoing from the <code>Goldweb</code> server.
<code>next_action markEF</code>	Instructs the <code>ipgpc</code> module to pass packets of the <code>video</code> class to the <code>markEF</code> statement after <code>ipgpc</code> completes processing. The <code>markEF</code> statement calls the <code>dscpmk</code> marker.
<code>enable_stats FALSE</code>	Enables statistics collection for the <code>video</code> class. However, because the value of <code>enable_stats</code> is <code>FALSE</code> , statistics collection for this class is not turned on.

- See Also**
- To define filters for the class you just created, refer to [“How to Define Filters in the IPQoS Configuration File”](#) on page 722.
 - To create another class clause for the configuration file, refer to [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

▼ How to Define Filters in the IPQoS Configuration File

The next procedure shows how to define filters for a class in the IPQoS configuration file.

- Before You Begin** The procedure assumes that you have already started file creation and have defined classes. The steps continue building the `/var/ipqos/Goldweb.qos` file that is created in [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

Note – As you create the IPQoS configuration file, be very careful to start and end each `class` clause and each `filter` clause with curly braces (`{ }`). For an example of the use of braces, use [Example 33–1](#).

- Steps** 1. **Open the IPQoS configuration file, and locate the end of the last class that you defined.**

For example, on the IPQoS-enabled server `Goldweb`, you would start after the following `class` clause in `/var/ipqos/Goldweb.qos`:

```
class {
    name video
    next_action markEF
    enable_stats FALSE
```

```
}
```

2. Define a filter clause to select outgoing traffic from the IPQoS system.

```
filter {  
    name webout  
    sport 80  
    direction LOCAL_OUT  
    class goldweb  
}
```

<code>name webout</code>	Gives the name <code>webout</code> to the filter.
<code>sport 80</code>	Selects traffic with a source port of 80, the well-known port for HTTP (web) traffic.
<code>direction LOCAL_OUT</code>	Further selects traffic that is outgoing from the local system.
<code>class goldweb</code>	Identifies the class to which the filter belongs, in this instance, class <code>goldweb</code> .

For syntactical and detailed information about the `filter` clause in the IPQoS configuration file, refer to [“filter Clause” on page 773](#).

3. Define a filter clause to select streaming video traffic on the IPQoS system.

```
filter {  
    name videoout  
    sport videosrv  
    direction LOCAL_OUT  
    class video  
}
```

<code>name videoout</code>	Gives the name <code>videoout</code> to the filter.
<code>sport videosrv</code>	Selects traffic with a source port of <code>videosrv</code> , a previously defined port for the streaming video application on this system.
<code>direction LOCAL_OUT</code>	Further selects traffic that is outgoing from the local system.
<code>class video</code>	Identifies the class to which the filter belongs, in this instance, class <code>video</code> .

- See Also**
- To define forwarding behaviors for the marker modules, refer to [“How to Define Traffic Forwarding in the IPQoS Configuration File” on page 724](#).
 - To define flow-control parameters for the metering modules, refer to [“How to Configure Flow Control in the IPQoS Configuration File” on page 737](#).
 - To activate the IPQoS configuration file, refer to [“How to Apply a New Configuration to the IPQoS Kernel Modules” on page 744](#).
 - To define additional filters, refer to [“How to Define Filters in the IPQoS Configuration File” on page 722](#).

- To create classes for traffic flows from applications, refer to “How to Configure the IPQoS Configuration File for an Application Server” on page 733.

▼ How to Define Traffic Forwarding in the IPQoS Configuration File

The next procedure shows how to define traffic forwarding by adding per-hop behaviors for a class into the IPQoS configuration file.

Before You Begin

The procedure assumes that you have an existing IPQoS configuration file with already defined classes and already defined filters. The steps continue building the `/var/ipqos/Goldweb.qos` file from [Example 33-1](#).

Note – The procedure shows how to configure traffic forwarding by using the `dscpmk` marker module. For information about traffic forwarding on VLAN systems by using the `d1closmk` marker, refer to “Using the `d1cosmk` Marker With VLAN Devices” on page 765.

Steps 1. Open the IPQoS configuration file, and locate the end of the last filter you defined.

For example, on the IPQoS-enabled server `Goldweb`, you would start after the following filter clause in `/var/ipqos/Goldweb.qos`:

```
filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}
}
```

Note that this `filter` clause is at the end of the `ipgpc` classifier action statement. Therefore, you need a closing brace to terminate the filter and a second closing brace to terminate the action statement.

2. Invoke the marker with the following action statement.

```
action {
    module dscpmk
    name markAF11
```

`module dscpmk` Calls the marker module `dscpmk`.

`name markAF11` Gives the name `markAF11` to the action statement.

The previously defined class `goldweb` includes a `next_action markAF11` statement. This statement sends traffic flows to the `markAF11` action statement after the classifier concludes processing.

3. Define actions for the marker to take on the traffic flow.

```

    params {
        global_stats FALSE
        dscp_map{0-63:10}
        next_action continue
    }
}

```

<code>global_stats FALSE</code>	Enables statistics collection for the <code>markAF11</code> marker action statement. However, because the value of <code>enable_stats</code> is <code>FALSE</code> , statistics are not collected.
<code>dscp_map{0-63:10}</code>	Assigns a DSCP of 10 to the packet headers of the traffic class <code>goldweb</code> , which is currently being processed by the marker.
<code>next_action continue</code>	Indicates that no further processing is required on packets of the traffic class <code>goldweb</code> , and that these packets can return to the network stream.

The DSCP of 10 instructs the marker to set all entries in the `dscp` map to the decimal value 10 (binary 001010). This codepoint indicates that packets of the `goldweb` traffic class are subject to the AF11 per-hop behavior. AF11 guarantees that all packets with the DSCP of 10 receive a low-drop, high-priority service. Thus, outgoing traffic for premium customers on `Goldweb` is given the highest priority that is available for the Assured Forwarding (AF) PHB. For a table of possible DSCPs for AF, refer to [Table 36-2](#).

4. Start another marker action statement.

```

action {
    module dscpmk
    name markEF
}

```

<code>module dscpmk</code>	Calls the marker module <code>dscpmk</code> .
<code>name markEF</code>	Gives the name <code>markEF</code> to the action statement.

5. Define actions for the marker to take on the traffic flow.

```

    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}

```

<code>global_stats TRUE</code>	Enables statistics collection on class <code>video</code> , which selects streaming video packets.
--------------------------------	--

<code>dscp_map{0-63:46}</code>	Assigns a DSCP of 46 to the packet headers of the traffic class <code>video</code> , which is currently being processed by the marker.
<code>next_action acct</code>	Instructs the <code>dscpmk</code> module to pass packets of the class <code>video</code> to the <code>acct</code> action statement after <code>dscpmk</code> completes processing. The <code>acct</code> action statement invokes the <code>flowacct</code> module.

The DSCP of 46 instructs the `dscpmk` module to set all entries in the `dscp` map to the decimal value 46 (binary 101110) in the DS field. This codepoint indicates that packets of the `video` traffic class are subject to the Expedited Forwarding (EF) per-hop behavior.

Note – The recommended codepoint for EF is 46 (binary 101110). Other DSCPs assign AF PHBs to a packet.

The EF PHB guarantees that packets with the DSCP of 46 are given the highest precedence by IPQoS and Diffserv-aware systems. Streaming applications require highest-priority service, which is the rationale behind assigning to streaming applications the EF PHBs in the QoS policy. For more details about the expedited forwarding PHB, refer to [“Expedited Forwarding \(EF\) PHB” on page 764](#).

6. Add the DSCPs that you have just created to the appropriate files on the Diffserv router.

For more information, refer to [“How to Configure a Router on an IPQoS-Enabled Network” on page 741](#).

- See Also**
- To start gathering flow-accounting statistics on traffic flows, refer to [“How to Enable Accounting for a Class in the IPQoS Configuration File” on page 727](#).
 - To define forwarding behaviors for the marker modules, refer to [“How to Define Traffic Forwarding in the IPQoS Configuration File” on page 724](#).
 - To define flow-control parameters for the metering modules, refer to [“How to Configure Flow Control in the IPQoS Configuration File” on page 737](#).
 - To activate the IPQoS configuration file, refer to [“How to Apply a New Configuration to the IPQoS Kernel Modules” on page 744](#).
 - To define additional filters, refer to [“How to Define Filters in the IPQoS Configuration File” on page 722](#).
 - To create classes for traffic flows from applications, refer to [“How to Configure the IPQoS Configuration File for an Application Server” on page 733](#).

▼ How to Enable Accounting for a Class in the IPQoS Configuration File

The next procedure shows how to enable accounting on a traffic class in the IPQoS configuration file. The procedure shows how to define flow accounting for the video class, which is introduced in “[How to Create the IPQoS Configuration File and Define Traffic Classes](#)” on page 720. This class selects streaming video traffic, which must be billed as part of a premium customer’s SLA.

Before You Begin The procedure assumes that you have an existing IPQoS configuration file with already defined classes, filters, metering actions, if appropriate, and marking actions, if appropriate. The steps continue building the `/var/ipqos/Goldweb.qos` file from [Example 33-1](#).

- Steps** 1. **Open the IPQoS configuration file, and locate the end of the last action statement you defined.**

For example, on the IPQoS-enabled server `Goldweb`, you would start after the following `markEF` action statement in `/var/ipqos/Goldweb.qos`.

```
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

2. **Begin an action statement that calls flow accounting.**

```
action {
    module flowacct
    name acct
```

`module flowacct` Invokes the flow-accounting module `flowacct`.

`name acct` Gives the name `acct` to the action statement

3. **Define a `params` clause to control accounting on the traffic class.**

```
params {
    global_stats TRUE
    timer 10000
    timeout 10000
    max_limit 2048
    next_action continue
}
}
```

<code>global_stats TRUE</code>	Enables statistics collection on the class <code>video</code> , which selects streaming video packets.
<code>timer 10000</code>	Specifies the duration of the interval, in milliseconds, when the flow table is scanned for timed-out flows. In this parameter, that interval is 10000 milliseconds.
<code>timeout 10000</code>	Specifies the minimum interval timeout value. A flow “times out” when packets for the flow are not seen during a time out interval. In this parameter, packets time out after 10000 milliseconds.
<code>max_limit 2048</code>	Sets the maximum number of active flow records in the flow table for this action instance.
<code>next_action continue</code>	Indicates that no further processing is required on packets of the traffic class <code>video</code> , and that these packets can return to the network stream.

The `flowacct` module gathers statistical information on packet flows of a particular class until a specified `timeout` value is reached.

- See Also**
- To configure per-hop behaviors on a router, refer to [“How to Configure a Router on an IPQoS-Enabled Network”](#) on page 741.
 - To activate the IPQoS configuration file, refer to [“How to Apply a New Configuration to the IPQoS Kernel Modules”](#) on page 744.
 - To create classes for traffic flows from applications, refer to [“How to Configure the IPQoS Configuration File for an Application Server”](#) on page 733.

▼ How to Create an IPQoS Configuration File for a Best-Effort Web Server

The IPQoS configuration file for a best-effort web server differs slightly from an IPQoS configuration file for a premium web server. As an example, the procedure uses the configuration file from [Example 33-2](#).

- Steps**
1. Log in to the best-effort web server.
 2. Create a new IPQoS configuration file with a `.qos` extension.

```

fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
}

```


The `/var/ipqos/userweb.qos` file must begin with the partial `action` statement to invoke the `ipgpc` classifier. In addition, the `action` statement also has a `params` clause to turn on statistics collection. For an explanation of this `action` statement, see [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

3. Define a class that identifies traffic that is bound for the best-effort web server.

```
class {
    name userweb
    next_action markAF12
    enable_stats FALSE
}
```

<code>name userweb</code>	Creates a class that is called <code>userweb</code> for forwarding web traffic from users.
<code>next_action markAF1</code>	Instructs the <code>ipgpc</code> module to pass packets of the <code>userweb</code> class to the <code>markAF12</code> <code>action</code> statement after <code>ipgpc</code> completes processing. The <code>markAF12</code> <code>action</code> statement invokes the <code>dscpmk</code> marker.
<code>enable_stats FALSE</code>	Enables statistics collection for the <code>userweb</code> class. However, because the value of <code>enable_stats</code> is <code>FALSE</code> , statistics collection for this class does not occur.

For an explanation of the `class` clause task, see [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

4. Define a filter clause to select traffic flows for the `userweb` class.

```
filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class userweb
}
}
```

<code>name webout</code>	Gives the name <code>webout</code> to the filter.
<code>sport 80</code>	Selects traffic with a source port of 80, the well-known port for HTTP (web) traffic.
<code>direction LOCAL_OUT</code>	Further selects traffic that is outgoing from the local system.
<code>class userweb</code>	Identifies the class to which the filter belongs, in this instance, class <code>userweb</code> .

For an explanation of the `filter` clause task, see [“How to Define Filters in the IPQoS Configuration File”](#) on page 722.

5. **Begin the action statement to invoke the dscpmk marker.**

```
action {  
    module dscpmk  
    name markAF12
```

module dscpmk Invokes the marker module dscpmk.

name markAF12 Gives the name markAF12 to the action statement.

The previously defined class userweb includes a next_action markAF12 statement. This statement sends traffic flows to the markAF12 action statement after the classifier concludes processing.

6. **Define parameters for the marker to use for processing the traffic flow.**

```
    params {  
        global_stats FALSE  
        dscp_map{0-63:12}  
        next_action continue  
    }  
}
```

global_stats Enables statistics collection for the markAF12 marker
FALSE action statement. However, because the value of
enable_stats is FALSE, statistics collection does not
occur.

dscp_map{0-63:12} Assigns a DSCP of 12 to the packet headers of the traffic
class userweb, which is currently being processed by the
marker.

next_action continue Indicates that no further processing is required on packets
of the traffic class userweb, and that these packets can
return to the network stream.

The DSCP of 12 instructs the marker to set all entries in the dscp map to the decimal value 12 (binary 001100). This codepoint indicates that packets of the userweb traffic class are subject to the AF12 per-hop behavior. AF12 guarantees that all packets with the DSCP of 12 in the DS field receive a medium-drop, high-priority service.

7. **When you complete the IPQoS configuration file, apply the configuration.**

- See Also**
- To add classes and other configuration for traffic flows from applications, refer to [“How to Configure the IPQoS Configuration File for an Application Server”](#) on page 733.
 - To configure per-hop behaviors on a router, refer to [“How to Configure a Router on an IPQoS-Enabled Network”](#) on page 741.
 - To activate your IPQoS configuration file, refer to [“How to Apply a New Configuration to the IPQoS Kernel Modules”](#) on page 744.

Creating an IPQoS Configuration File for an Application Server

This section explains how to create a configuration file for an application server that provides major applications to customers. The procedure uses as its example the BigAPPS server from [Figure 32-4](#).

The following configuration file defines IPQoS activities for the BigAPPS server. This server hosts FTP, electronic mail (SMTP), and network news (NNTP) for customers.

EXAMPLE 33-3 Sample IPQoS Configuration File for an Application Server

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        next_action meterftp
    }
    filter {
        name smtpout
        sport smtp
        class smtp
    }
    filter {
        name newsout
        sport nntp
        class news
    }
    filter {
        name ftpout
        sport ftp
        class ftp
    }
    filter {
```

EXAMPLE 33-3 Sample IPQoS Configuration File for an Application Server (Continued)

```
        name ftpdata
        sport ftp-data
        class ftp
    }
}
action {
    module dscpmk
    name markAF13
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
action {
    module tokenmt
    name meterftp
    params {
        committed_rate 50000000
        committed_burst 50000000
        red_action_name AF31
        green_action_name markAF22
        global_stats TRUE
    }
}
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

```
}
```

▼ How to Configure the IPQoS Configuration File for an Application Server

- Steps** 1. Log in to the IPQoS-enabled application server, and create a new IPQoS configuration file with a `.qos` extension.

For example, you would create the `/var/ipqos/BigAPPS.qos` file for the application server. Begin with the following required phrases to start the `action` statement that invokes the `ipgpc` classifier:

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
}
```

For an explanation of the opening `action` statement, refer to “How to Create the IPQoS Configuration File and Define Traffic Classes” on page 720.

2. Create classes to select traffic from three applications on the BigAPPS server.

Add the class definitions after the opening `action` statement.

```
class {
    name smtp
    enable_stats FALSE
    next_action markAF13
}
class {
    name news
    next_action markAF21
}
class {
    name ftp
    enable_stats TRUE
    next_action meterftp
}
```

```
name smtp
```

Creates a class that is called `smtp`, which includes email traffic flows to be handled by the SMTP application

<code>enable_stats FALSE</code>	Enables statistics collection for the <code>smtp</code> class. However, because the value of <code>enable_stats</code> is <code>FALSE</code> , statistics for this class are not taken.
<code>next_action markAF13</code>	Instructs the <code>ipgpc</code> module to pass packets of the <code>smtp</code> class to the <code>markAF13</code> action statement after <code>ipgpc</code> completes processing.
<code>name news</code>	Creates a class that is called <code>news</code> , which includes network news traffic flows to be handled by the NNTTP application.
<code>next_action markAF21</code>	Instructs the <code>ipgpc</code> module to pass packets of the <code>news</code> class to the <code>markAF21</code> action statement after <code>ipgpc</code> completes processing.
<code>name ftp</code>	Creates a class that is called <code>ftp</code> , which handles outgoing traffic that is handled by the FTP application.
<code>enable_stats TRUE</code>	Enables statistics collection for the <code>ftp</code> class.
<code>next_action meterftp</code>	Instructs the <code>ipgpc</code> module to pass packets of the <code>ftp</code> class to the <code>meterftp</code> action statement after <code>ipgpc</code> completes processing.

For more information about defining classes, refer to [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.

3. Define filter clauses to select traffic of the classes defined in Step 2.

```

filter {
    name smtpout
    sport smtp
    class smtp
}
filter {
    name newsout
    sport nntp
    class news
}
filter {
    name ftpout
    sport ftp
    class ftp
}
filter {
    name ftpdata
    sport ftp-data
    class ftp
}
}

name smtpout          Gives the name smtpout to the filter.

```

<code>sport smtp</code>	Selects traffic with a source port of 25, the well-known port for the <code>sendmail</code> (SMTP) application.
<code>class smtp</code>	Identifies the class to which the filter belongs, in this instance, <code>class smtp</code> .
<code>name newsout</code>	Gives the name <code>newsout</code> to the filter.
<code>sport nntp</code>	Selects traffic with a source port name of <code>nntp</code> , the well-known port name for the network news (NNTP) application.
<code>class news</code>	Identifies the class to which the filter belongs, in this instance, <code>class news</code> .
<code>name ftpout</code>	Gives the name <code>ftpout</code> to the filter.
<code>sport ftp</code>	Selects control data with a source port of 21, the well-known port number for FTP traffic.
<code>name ftpdata</code>	Gives the name <code>ftpdata</code> to the filter.
<code>sport ftp-data</code>	Selects traffic with a source port of 20, the well-known port number for FTP data traffic.
<code>class ftp</code>	Identifies the class to which the <code>ftpout</code> and <code>ftpdata</code> filters belong, in this instance <code>ftp</code> .

- See Also**
- To define filters, refer to “[How to Define Filters in the IPQoS Configuration File](#)” on page 722.
 - To define forwarding behaviors for application traffic, refer to “[How to Configure Forwarding for Application Traffic in the IPQoS Configuration File](#)” on page 735.
 - To configure flow control by using the metering modules, refer to “[How to Configure Flow Control in the IPQoS Configuration File](#)” on page 737.
 - To configure flow accounting, refer to “[How to Enable Accounting for a Class in the IPQoS Configuration File](#)” on page 727.

▼ How to Configure Forwarding for Application Traffic in the IPQoS Configuration File

The next procedure shows how to configure forwarding for application traffic. In the procedure, you define per-hop behaviors for application traffic classes that might have lower precedence than other traffic on a network. The steps continue building the `/var/ipqos/BigAPPS.qos` file in [Example 33-3](#).

- Before You Begin** The procedure assumes that you have an existing IPQoS configuration file with already-defined classes and already-defined filters for the applications to be marked.

- Steps** 1. Open the IPQoS configuration file that you have created for the application server, and locate the end of the last `filter` clause.

In the `/var/ipqos/BigAPPS.qos` file, the last filter is the following:

```
filter {
    name ftpdata
    sport ftp-data
    class ftp
}
}
```

2. Invoke the marker as follows:

```
action {
    module dscpmk
    name markAF13
}
```

`module dscpmk` Invokes the marker module `dscpmk`.

`name markAF13` Gives the name `markAF13` to the action statement.

3. Define the per-hop behavior to be marked on electronic mail traffic flows.

```
params {
    global_stats FALSE
    dscp_map{0-63:14}
    next_action continue
}
}
```

`global_stats FALSE` Enables statistics collection for the `markAF13` marker action statement. However, because the value of `enable_stats` is `FALSE`, statistics are not collected.

`dscp_map{0-63:14}` Assigns a DSCP of 14 to the packet headers of the traffic class `smtp`, which is currently being processed by the marker.

`next_action continue` Indicates that no further processing is required on packets of the traffic class `smtp`. These packets can then return to the network stream.

The DSCP of 14 tells the marker to set all entries in the `dscp` map to the decimal value 14 (binary 001110). The DSCP of 14 sets the AF13 per-hop behavior. The marker marks packets of the `smtp` traffic class with the DSCP of 14 in the DS field.

AF13 assigns all packets with a DSCP of 14 to a high-drop precedence. However, because AF13 also assures a Class 1 priority, the router still guarantees outgoing email traffic a high priority in its queue. For a table of possible AF codepoints, refer to [Table 36-2](#).

4. Add a marker action statement to define a per-hop behavior for network news traffic:

```
action {
  module dscpmk
  name markAF21
  params {
    global_stats FALSE
    dscp_map{0-63:18}
    next_action continue
  }
}
```

`name markAF21` Gives the name markAF21 to the action statement.

`dscp_map{0-63:18}` Assigns a DSCP of 18 to the packet headers of the traffic class nntp, which is currently being processed by the marker.

The DSCP of 18 tells the marker to set all entries in the dscp map to the decimal value 18 (binary 010010). The DSCP of 18 sets the AF21 per-hop behavior. The marker marks packets of the news traffic class with the DSCP of 18 in the DS field.

AF21 assures that all packets with a DSCP of 18 receive a low-drop precedence, but with only Class 2 priority. Thus, the possibility of network news traffic being dropped is low.

- See Also**
- To add configuration information for web servers, refer to [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.
 - To configure flow control by using the metering modules, refer to [“How to Configure Flow Control in the IPQoS Configuration File”](#) on page 737.
 - To configure flow accounting, refer to [“How to Enable Accounting for a Class in the IPQoS Configuration File”](#) on page 727.
 - To configure forwarding behaviors on a router, refer to [“How to Configure a Router on an IPQoS-Enabled Network”](#) on page 741.
 - To activate the IPQoS configuration file, refer to [“How to Apply a New Configuration to the IPQoS Kernel Modules”](#) on page 744.

▼ How to Configure Flow Control in the IPQoS Configuration File

To control the rate at which a particular traffic flow is released onto the network, you must define parameters for the meter. You can use either of the two meter modules, `tokenmt` or `tswtclmt`, in the IPQoS configuration file.

The next procedure continues to build the IPQoS configuration file for the application server in [Example 33–3](#). In the procedure, you configure not only the meter but also two marker actions that are called within the meter `action` statement.

Before You Begin The steps assume that you have already defined a class and a filter for the application to be flow-controlled.

Steps 1. **Open the IPQoS configuration file that you have created for the applications server.**

In the `/var/ipqos/BigAPPS.qos` file, you begin after the following marker action:

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

2. **Create a meter action statement to flow-control traffic of the ftp class.**

```
action {
    module tokenmt
    name meterftp
```

`module tokenmt` Invokes the `tokenmt` meter.

`name meterftp` Gives the name `meterftp` to the action statement.

3. **Add parameters to configure the meter's rate.**

```
params {
    committed_rate 50000000
    committed_burst 50000000
```

`committed_rate 50000000` Assigns a transmission rate of 50,000,000 bps to traffic of the `ftp` class.

`committed_burst 50000000` Commits a burst size of 50,000,000 bits to traffic of the `ftp` class.

For an explanation of `tokenmt` parameters, refer to [“Configuring tokenmt as a Two-Rate Meter”](#) on page 761.

4. **Add parameters to configure traffic conformance precedences:**

```
red_action markAF31
green_action_name markAF22
global_stats TRUE
}
}
```

<code>red_action_name markAF31</code>	Indicates that when the traffic flow of the <code>ftp</code> class exceeds the committed rate, packets are sent to the <code>markAF31</code> marker action statement.
<code>green_action_name markAF22</code>	Indicates that when traffic flows of class <code>ftp</code> conform to the committed rate, packets are sent to the <code>markAF22</code> action statement.
<code>global_stats TRUE</code>	Enables metering statistics for the <code>ftp</code> class. For more information about traffic conformance, see “Meter Module” on page 760 .

5. Add a marker action statement to assign a per-hop behavior to nonconformant traffic flows of class `ftp`.

```

action {
  module dscpmk
  name markAF31
  params {
    global_stats TRUE
    dscp_map{0-63:26}
    next_action continue
  }
}

```

<code>module dscpmk</code>	Invokes the marker module <code>dscpmk</code> .
<code>name markAF31</code>	Gives the name <code>markAF31</code> to the action statement.
<code>global_stats TRUE</code>	Enables statistics for the <code>ftp</code> class.
<code>dscp_map{0-63:26}</code>	Assigns a DSCP of 26 to the packet headers of the traffic class <code>ftp</code> whenever this traffic exceeds the committed rate.
<code>next_action continue</code>	Indicates that no further processing is required on packets of the traffic class <code>ftp</code> . Then these packets can return to the network stream.

The DSCP of 26 instructs the marker to set all entries in the `dscp` map to the decimal value 26 (binary 011010). The DSCP of 26 sets the AF31 per-hop behavior. The marker marks packets of the `ftp` traffic class with the DSCP of 26 in the DS field.

AF31 assures that all packets with a DSCP of 26 receive a low-drop precedence, but with only Class 3 priority. Therefore, the possibility of nonconformant FTP traffic being dropped is low. For a table of possible AF codepoints, refer to [Table 36-2](#).

6. Add a marker `action` statement to assign a per-hop behavior to `ftp` traffic flows that conform to the committed rate.

```
action {
  module dscpmk
  name markAF22
  params {
    global_stats TRUE
    dscp_map{0-63:20}
    next_action continue
  }
}
```

`name markAF22` Gives the name `markAF22` to the marker action.

`dscp_map{0-63:20}` Assigns a DSCP of 20 to the packet headers of the traffic class `ftp` whenever `ftp` traffic conforms to its configured rate.

The DSCP of 20 tells the marker to set all entries in the `dscp map` to the decimal value 20 (binary 010100). The DSCP of 20 sets the AF22 per-hop behavior. The marker marks packets of the `ftp` traffic class with the DSCP of 20 in the DS field.

AF22 assures that all packets with a DSCP of 20 receive a medium-drop precedence with Class 2 priority. Therefore, conformant FTP traffic is assured a medium-drop precedence among flows that are simultaneously released by the IPQoS system. However, the router gives a higher forwarding priority to traffic classes with a Class 1 medium-drop precedence mark or higher. For a table of possible AF codepoints, refer to [Table 36-2](#).

7. Add the DSCPs that you have created for the application server to the appropriate files on the Diffserv router.

- See Also**
- To activate the IPQoS configuration file, refer to [“How to Apply a New Configuration to the IPQoS Kernel Modules”](#) on page 744.
 - To add configuration information for web servers, refer to [“How to Create the IPQoS Configuration File and Define Traffic Classes”](#) on page 720.
 - To configure flow accounting, refer to [“How to Enable Accounting for a Class in the IPQoS Configuration File”](#) on page 727.
 - To configure forwarding behaviors on a router, refer to [“How to Configure a Router on an IPQoS-Enabled Network”](#) on page 741.

Providing Differentiated Services on a Router

To provide true differentiated services, you must include a Diffserv-aware router in your network topology, as described in “[Hardware Strategies for the Diffserv Network](#)” on page 696. The actual steps for configuring Diffserv on a router and updating that router’s files are outside the scope of this guide.

This section gives general steps for coordinating the forwarding information among various IPQoS-enabled systems on the network and the Diffserv router.

▼ How to Configure a Router on an IPQoS-Enabled Network

The next procedure uses as its example the topology in [Figure 32-4](#).

Before You Begin The next procedure assumes that you have already configured the IPQoS systems on your network by performing the previous tasks in this chapter.

- Steps**
1. **Review the configuration files for all IPQoS-enabled systems on your network.**
 2. **Identify each codepoint that is used in the QoS various policies.**

List the codepoints, and the systems and classes, to which the codepoints apply. The next table can illustrate areas where you might have used the same codepoint. This practice is acceptable. However, you should provide other criteria in the IPQoS configuration file, such as a precedence selector, to determine the precedence of identically marked classes.

For example, for the sample network that is used in the procedures throughout this chapter, you might construct the following codepoint table.

System	Class	PHB	DS Codepoint
Goldweb	video	EF	46 (101110)
Goldweb	goldweb	AF11	10 (001010)
Userweb	webout	AF12	12 (001100)
BigAPPS	smtp	AF13	14 (001110)
BigAPPS	news	AF18	18 (010010)

System	Class	PHB	DS Codepoint
BigAPPS	ftp conformant traffic	AF22	20 (010100)
BigAPPS	ftp nonconformant traffic	AF31	26 (011010)

3. Add the codepoints from your network's IPQoS configuration files to the appropriate files on the Diffserv router.

The codepoints that you supply should help to configure the router's Diffserv scheduling mechanism. Refer to the router manufacturer's documentation and web sites for instructions.

Starting and Maintaining IPQoS (Tasks)

This chapter contains tasks for activating an IPQoS configuration file and for logging IPQoS-related events. The following topics are covered:

- “Administering IPQoS (Task Map)” on page 743
- “Applying an IPQoS Configuration” on page 744
- “Enabling `syslog` Logging for IPQoS Messages” on page 746
- “Troubleshooting with IPQoS Error Messages” on page 747

Administering IPQoS (Task Map)

This section lists the set of tasks for starting and maintaining IPQoS on a Solaris system. Before you use the tasks, you must have a completed IPQoS configuration file, as described in “Defining a QoS Policy in the IPQoS Configuration File (Task Map)” on page 715.

Task	Description	For Instructions
1. Configure IPQoS on a system.	Use the <code>ipqosconf</code> command to activate the IPQoS configuration file on a system.	“How to Apply a New Configuration to the IPQoS Kernel Modules” on page 744
2. Make the Solaris startup scripts apply the debugged IPQoS configuration file after each system boot.	Ensure that the IPQoS configuration is applied each time the system reboots.	“How to Ensure That the IPQoS Configuration Is Applied After Each Reboot” on page 745.
3. Enable <code>syslog</code> logging for IPQoS.	Add an entry to enable <code>syslog</code> logging of IPQoS messages.	“How to Enable Logging of IPQoS Messages During Booting” on page 746.

Task	Description	For Instructions
4. Fix any IPQoS problems that arise.	Troubleshoot IPQoS problems by using error messages.	Refer to the error messages in Table 34-1 .

Applying an IPQoS Configuration

You activate and otherwise manipulate the IPQoS configuration by using the `ipqosconf` command.

▼ How to Apply a New Configuration to the IPQoS Kernel Modules

You use the `ipqosconf` command to read the IPQoS configuration file and to configure the IPQoS modules in the UNIX kernel. The next procedure uses as an example the file `/var/ipqos/Goldweb.qos`, which is created in [“Creating IPQoS Configuration Files for Web Servers”](#) on page 718. For detailed information, refer to the `ipqosconf(1M)` man page.

Steps 1. Assume the Primary Administrator role, or become superuser, on the IPQoS-enabled system.

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. Apply the new configuration.

```
# /usr/sbin/ipqosconf -a /var/ipqos/Goldweb.qos
```

`ipqosconf` writes the information in the specified IPQoS configuration file into the IPQoS modules in the Solaris kernel. In this example, the contents of `/var/ipqos/Goldweb.qos` are applied to the current Solaris kernel.

Note – When you apply an IPQoS configuration file with the `-a` option, the actions in the file are active for the current session only.

3. Test and debug the new IPQoS configuration.

Use UNIX utilities to track IPQoS behavior and to gather statistics on your IPQoS implementation. This information can help you determine if the configuration operates as expected.

- See Also**
- To view statistics on how IPQoS modules are working, refer to [“Gathering Statistical Information”](#) on page 754.
 - To log `ipqosconf` messages, refer to [“Enabling syslog Logging for IPQoS Messages”](#) on page 746.
 - To ensure that the current IPQoS configuration is applied after each boot, refer to [“How to Ensure That the IPQoS Configuration Is Applied After Each Reboot”](#) on page 745.

▼ How to Ensure That the IPQoS Configuration Is Applied After Each Reboot

You must explicitly make an IPQoS configuration persistent across reboots. Otherwise, the current configuration applies only until the system reboots. When IPQoS works correctly on a system, do the following to make the configuration persistent across reboots.

- Steps**
1. **Assume the Primary Administrator role, or become superuser, on the IPQoS-enabled system.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, *“Working With the Solaris Management Console (Tasks),”* in *System Administration Guide: Basic Administration*.

2. **Test for the existence of an IPQoS configuration in the kernel modules.**

```
# ipqosconf -l
```

If a configuration already exists, `ipqosconf` displays the configuration on the screen. If you do not receive output, apply the configuration, as explained in [“How to Apply a New Configuration to the IPQoS Kernel Modules”](#) on page 744.

3. **Ensure that the existing IPQoS configuration is applied every time the IPQoS system reboots.**

```
# /usr/sbin/ipqosconf -c
```

The `-c` option causes the current IPQoS configuration to be represented in the boot-time configuration file `/etc/inet/ipqosinit.conf`.

Enabling syslog Logging for IPQoS Messages

To record IPQoS boot-time messages, you need to modify the `/etc/syslog.conf` file as shown in the next procedure.

▼ How to Enable Logging of IPQoS Messages During Booting

- Steps**
1. **Assume the Primary Administrator role, or become superuser, on the IPQoS-enabled system.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Open the `/etc/syslog.conf` file.**
3. **Add the following text as the final entry in the file.**

```
user.info                /var/adm/messages
```

Use tabs rather than spaces between the columns.

The entry logs all boot-time messages that are generated by IPQoS into the `/var/adm/messages` file.

4. **Reboot the system to apply the messages.**

Example 34–1 IPQoS Output From `/var/adm/messages`

When you view `/var/adm/messages` after system reboot, your output might contain IPQoS logging messages that are similar to the following.

```
May 14 10:44:33 ipqos-14 ipqosconf: [ID 815575 user.info]
  New configuration applied.
May 14 10:44:46 ipqos-14 ipqosconf: [ID 469457 user.info]
  Current configuration saved to init file.
May 14 10:44:55 ipqos-14 ipqosconf: [ID 435810 user.info]
  Configuration flushed.
```

You might also see IPQoS error messages that are similar to the following in your IPQoS system's `/var/adm/messages` file.

```
May 14 10:56:47 ipqos-14 ipqosconf: [ID 123217 user.error]
  Missing/Invalid config file fmt_version.
```

```
May 14 10:58:19 ipqos-14 ipqosconf: [ID 671991 user.error]
No ipgpc action defined.
```

For a description of these error messages, see [Table 34-1](#).

Troubleshooting with IPQoS Error Messages

This section contains a table of error messages that are generated by IPQoS and their possible solutions.

TABLE 34-1 IPQoS Error Messages

Error Message	Description	Solution
Undefined action in parameter <i>parameter-name</i> 's action <i>action-name</i>	In the IPQoS configuration file, the action name that you specified in <i>parameter-name</i> does not exist in the configuration file.	Create the action. Or, refer to a different, existing action in the parameter.
action <i>action-name</i> involved in cycle	In the IPQoS configuration file, <i>action-name</i> is part of a cycle of actions, which is not allowed by IPQoS.	Determine the action cycle. Then remove one of the cyclical references from the IPQoS configuration file.
Action <i>action-name</i> isn't referenced by any other actions	A non-ipgpc action definition is not referenced by any other defined actions in the IPQoS configuration, which is not allowed by IPQoS.	Remove the unreferenced action. Alternatively, make another action reference the currently unreferenced action.
Missing/Invalid config file <i>fmt_version</i>	The format of the configuration file is not specified as the first entry of the file, which is required by IPQoS.	Add the format version, as explained in "How to Create the IPQoS Configuration File and Define Traffic Classes" on page 720.
Unsupported config file format version	The format version that is specified in the configuration file is not supported by IPQoS.	Change the format version to <i>fmt_version 1.0</i> , which is required to run the Solaris 9 9/02 and later versions of IPQoS.
No ipgpc action defined.	You did not define an action for the ipgpc classifier in the configuration file, which is an IPQoS requirement.	Define an action for ipgpc, as shown in "How to Create the IPQoS Configuration File and Define Traffic Classes" on page 720.

TABLE 34-1 IPQoS Error Messages (Continued)

Error Message	Description	Solution
Can't commit a null configuration	When you ran <code>ipqosconf -c</code> to commit a configuration, that configuration was empty, which IPQoS does not allow.	Be sure to apply a configuration file before you attempt to commit a configuration. For instructions, see “How to Apply a New Configuration to the IPQoS Kernel Modules” on page 744.
Invalid CIDR mask on line <i>line-number</i>	In the configuration file, you used a CIDR mask as part of the IP address that is out of the valid range for IP addresses.	Change the mask value to be in the range of 1–32 for IPv4 and 1–128 for IPv6.
Address masks aren't allowed for host names line <i>line-number</i>	In the configuration file, you defined a CIDR mask for a host name, which is not allowed in IPQoS.	Remove the mask or change the host name to an IP address.
Invalid module name line <i>line-number</i>	In the configuration file, the module name that you specified in an action statement is invalid.	Check the spelling of the module name. For a list of IPQoS modules, refer to Table 36-5 .
ipgpc action has incorrect name line <i>line-number</i>	The name that you gave to the <code>ipgpc</code> action in the configuration file is not the required <code>ipgpc.classify</code> .	Rename the action <code>ipgpc.classify</code> .
Second parameter clause not supported line <i>line-number</i>	In the configuration file, you specified two parameter clauses for a single action, which IPQoS does not allow.	Combine all parameters for the action into a single parameters clause.
Duplicate named action	In the configuration file, you gave the same name to two actions.	Rename or remove one of the actions.
Duplicate named filter/class in action <i>action-name</i>	You gave the same name to two filters or two classes in the same action, which is not allowed in the IPQoS configuration file.	Rename or remove one of the filters or classes.
Undefined class in filter <i>filter-name</i> in action <i>action-name</i>	In the configuration file, the filter references a class that is not defined in the action.	Create the class, or change the filter reference to an already existing class.
Undefined action in class <i>class-name</i> action <i>action-name</i>	The class refers to an action that is not defined in the configuration file.	Create the action, or change the reference to an already existing action.
Invalid parameters for action <i>action-name</i>	In the configuration file, one of the parameters is invalid.	For the module that is called by the named action, refer to the module entry in “IPQoS Architecture and the Diffserv Model” on page 757. Alternatively, you can refer to the <code>ipqosconf(1M)</code> man page.

TABLE 34-1 IPQoS Error Messages (Continued)

Error Message	Description	Solution
Mandatory parameter missing for action <i>action-name</i>	You have not defined a required parameter for an action in the configuration file.	For the module that is called by the named action, refer to the module entry in “IPQoS Architecture and the Diffserv Model” on page 757. Alternatively, you can refer to the <code>ipqosconf(1M)</code> man page.
Max number of classes reached in <code>ipgpc</code>	You specified more classes than are allowed in the <code>ipgpc</code> action of the IPQoS configuration file. The maximum number is 10007.	Review the configuration file, and remove unneeded classes. Alternatively, you can raise the maximum number of classes by adding to the <code>/etc/system</code> file the entry <code>ipgpc_max_classesclass-number</code> .
Max number of filters reached in action <code>ipgpc</code>	You specified more filters than are allowed in the <code>ipgpc</code> action of the IPQoS configuration file. The maximum number is 10007.	Review the configuration file, and remove unneeded filters. Alternatively, you can raise the maximum number of filters by adding to the <code>/etc/system</code> file the entry <code>ipgpc_max_filtersfilter-number</code> .
Invalid/missing parameters for filter <i>filter-name</i> in action <code>ipgpc</code>	In the configuration file, filter <i>filter-name</i> has an invalid or missing parameter.	Refer to the <code>ipqosconf(1M)</code> man page for the list of valid parameters.
Name not allowed to start with '!', line <i>line-number</i>	You began an action, filter, or class name with an exclamation mark (!), which is not allowed in the IPQoS file.	Remove the exclamation mark, or rename the action, class, or filter.
Name exceeds the maximum name length <i>line-number</i>	You defined a name for an action, class, or filter in the configuration file that exceeds the maximum length of 23 characters.	Give a shorter name to the action, class, or filter.
Array declaration line <i>line-number</i> is invalid	In the configuration file, the array declaration for the parameter on line <i>line-number</i> is invalid.	For the correct syntax of the array declaration that is called by the <code>action</code> statement with the invalid array, refer to “IPQoS Architecture and the Diffserv Model” on page 757. Alternatively, refer to the <code>ipqosconf(1M)</code> man page.
Quoted string exceeds line, <i>line-number</i>	The string does not have the terminating quotation marks on the same line, which is required in the configuration file.	Make sure that the quoted string begins and ends on the same line in the configuration file.

TABLE 34-1 IPQoS Error Messages (Continued)

Error Message	Description	Solution
Invalid value, line <i>line-number</i>	The value that is given on <i>line-number</i> of the configuration file is not supported for the parameter.	For the acceptable values for the module that is called by the <code>action</code> statement, refer to the module description in “IPQoS Architecture and the Diffserv Model” on page 757. Alternatively, you can refer to the <code>ipqosconf(1M)</code> man page.
Unrecognized value, line <i>line-number</i>	The value on <i>line-number</i> of the configuration file is not a supported enumeration value for its parameter.	Check that the enumeration value is correct for the parameter. For a description of the module that is called by the <code>action</code> statement with the unrecognized line number, refer to “IPQoS Architecture and the Diffserv Model” on page 757. Alternatively, you can refer to the <code>ipqosconf(1M)</code> man page.
Malformed value list line <i>line-number</i>	The enumeration that is specified on <i>line-number</i> of the configuration file does not conform to the specification syntax.	For correct syntax for the module that is called by the <code>action</code> statement with the malformed value list, refer to the module description in “IPQoS Architecture and the Diffserv Model” on page 757. Alternatively, you can refer to the <code>ipqosconf(1M)</code> man page.
Duplicate parameter line <i>line-number</i>	A duplicate parameter was specified on <i>line-number</i> , which is not allowed in the configuration file.	Remove one of the duplicate parameters.
Invalid action name line <i>line-number</i>	You gave the action on <i>line-number</i> of the configuration file a name that uses the predefined name “continue” or “drop.”	Rename the action so that the action does not use a predefined name.
Failed to resolve src/dst host name for filter at line <i>line-number</i> , ignoring filter	<code>ipqosconf</code> could not resolve the source or destination address that was defined for the given filter in the configuration file. Therefore, the filter is ignored.	If the filter is important, try applying the configuration at a later time.
Incompatible address version line <i>line-number</i>	The IP version of the address on <i>line-number</i> is incompatible with the version of a previously specified IP address or <code>ip_version</code> parameter.	Change the two conflicting entries to be compatible.
Action at line <i>line-number</i> has the same name as currently installed action, but is for a different module	You tried to change the module of an action that already exists in the system’s IPQoS configuration, which is not allowed.	Flush the current configuration before you apply the new configuration.

Using Flow Accounting and Statistics Gathering (Tasks)

This chapter explains how to obtain accounting and statistical information on traffic that is handled by an IPQoS system. The following topics are discussed:

- “Setting Up Flow Accounting (Task Map)” on page 751
- “Recording Information About Traffic Flows” on page 752
- “Gathering Statistical Information” on page 754

Setting Up Flow Accounting (Task Map)

The following task map lists the generic tasks for obtaining information about traffic flows by using the `flowacct` module.

Task	Description	For Instructions
1. Create a file to contain accounting information for traffic flows.	Use the <code>acctadm</code> command to create a file that holds the results of processing by <code>flowacct</code> .	“How to Create a File for Flow-Accounting Data” on page 752
2. Define <code>flowacct</code> parameters in the IPQoS configuration file.	Define values for the <code>timer</code> , <code>timeout</code> , and <code>max_limit</code> parameters.	“How to Enable Accounting for a Class in the IPQoS Configuration File” on page 727

Recording Information About Traffic Flows

You use the IPQoS `flowacct` module to collect information about traffic flows. For example, you can collect source and destination addresses, number of packets in a flow, and similar data. The process of accumulating and recording information about flows is called *flow accounting*.

The results of flow accounting on traffic of a particular class are recorded in a table of *flow records*. Each flow record consists of a series of attributes. These attributes contain data about traffic flows of a particular class over an interval of time. For a list of the `flowacct` attributes, refer to [Table 36-4](#).

Flow accounting is particularly useful for billing clients as is defined in their service-level agreements (SLAs). You can also use flow accounting to obtain flow statistics for critical applications. This section contains tasks for using `flowacct` with the Solaris extended accounting facility to obtain data on traffic flows.

The following information is contained in sources outside this chapter:

- For instructions on creating an action statement for `flowacct` in the IPQoS configuration file, refer to [“How to Configure Flow Control in the IPQoS Configuration File”](#) on page 737.
- To learn how `flowacct` works, refer to [“Classifier Module”](#) on page 758.
- For technical information, refer to the `flowacct(7ipp)` man page.

▼ How to Create a File for Flow-Accounting Data

Before you add a `flowacct` action to the IPQoS configuration file, you must create a file for flow records from the `flowacct` module. You use the `acctadm` command for this purpose. `acctadm` can record either basic attributes or extended attributes in the file. All `flowacct` attributes are listed in [Table 36-4](#). For detailed information about `acctadm`, refer to the `acctadm(1M)` man page.

Steps 1. **Assume the Primary Administrator role, or become superuser, on the IPQoS-enabled system.**

The Primary Administrator role includes the Primary Administrator profile. To create the role and assign the role to a user, see Chapter 2, “Working With the Solaris Management Console (Tasks),” in *System Administration Guide: Basic Administration*.

2. **Create a basic flow-accounting file.**

The following example shows how to create a basic flow-accounting file for the premium web server that is configured in [Example 33-1](#).

```
# /usr/sbin/acctadm -e basic -f /var/ipqos/goldweb/account.info flow
```

acctadm -e	Invokes acctadm with the -e option. The -e option enables the arguments that follow.
basic	States that only data for the eight basic flowacct attributes is to be recorded in the file.
/var/ipqos/goldweb/account.info	Specifies the fully qualified path name of the file to hold the flow records from flowacct.
flow	Instructs acctadm to enable flow accounting.

3. View information about flow accounting on the IPQoS system by typing acctadm without arguments.

acctadm generates the following output:

```
Task accounting: inactive
    Task accounting file: none
    Tracked task resources: none
    Untracked task resources: extended
    Process accounting: inactive
    Process accounting file: none
    Tracked process resources: none
    Untracked process resources: extended,host,mstate
    Flow accounting: active
    Flow accounting file: /var/ipqos/goldweb/account.info
    Tracked flow resources: basic
    Untracked flow resources: dsfield,ctime,lseen,projid,uid
```

All entries but the last four are for use with the Solaris Resource Manager feature. The next table explains the entries that are specific to IPQoS.

Entry	Description
Flow accounting: active	Indicates that flow accounting is turned on.
Flow accounting file: /var/ipqos/goldweb/account.info	Gives the name of the current flow-accounting file.
Tracked flow resources: basic	Indicates that only the basic flow attributes are tracked.
Untracked flow resources: dsfield,ctime,lseen,projid,uid	Lists the flowacct attributes that are not tracked in the file.

4. (Optional) Add the extended attributes to the accounting file.

```
# acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

5. (Optional) Return to recording only the basic attributes in the accounting file.

```
# acctadm -d extended -e basic -f /var/ipqos/goldweb/account.info
```

The `-d` option disables extended accounting.

6. View the contents of a flow-accounting file.

Instructions for viewing the contents of a flow-accounting file are in “Perl Interface to libexacct” in *System Administration Guide: Solaris Containers—Resource Management and Solaris Zones*.

- See Also**
- For detailed information on the extended accounting feature, refer to Chapter 4, “Extended Accounting (Overview),” in *System Administration Guide: Solaris Containers—Resource Management and Solaris Zones*.
 - To define `flowacct` parameters in the IPQoS configuration file, refer to “How to Enable Accounting for a Class in the IPQoS Configuration File” on page 727.
 - To print the data in the file that was created with `acctadm`, refer to “Perl Interface to libexacct” in *System Administration Guide: Solaris Containers—Resource Management and Solaris Zones*.

Gathering Statistical Information

You can use the `kstat` command to generate statistical information from the IPQoS modules. Use the following syntax:

```
/bin/kstat -m ipqos-module-name
```

You can specify any valid IPQoS module name, as shown in Table 36–5. For example, to view statistics that are generated by the `dscpmk` marker, you use the following form of `kstat`:

```
/bin/kstat -m dscpmk
```

For technical details, refer to the `kstat(1M)` man page.

EXAMPLE 35–1 `kstat` Statistics for IPQoS

Here is an example of possible results from running `kstat` to obtain statistics about the `flowacct` module.

```
# kstat -m flowacct
module: flowacct                instance: 3
name:   Flowacct statistics     class:   flacct
        bytes_in_tbl            84
```

EXAMPLE 35-1 `kstat` Statistics for IPQoS (Continued)

```
      crtime                345728.504106363
      epackets              0
      flows_in_tbl         1
      nbytes                84
      npackets              1
      snaptime              345774.031843301
      usedmem               256
```

`class: flacct` Gives the name of the class to which the traffic flows belong, in this example `flacct`.

`bytes_in_tbl` Total number of bytes in the flow table. The total number of bytes is the sum in bytes of all the flow records that currently reside in the flow table. The total number of bytes for this flow table is 84. If no flows are in the table, the value for `bytes_in_tbl` is 0.

`crtime` The last time that this `kstat` output was created.

`epackets` Number of packets that resulted in an error during processing, in this example 0.

`flows_in_tbl` Number of flow records in the flow table, which in this example is 1. When no records are in the table, the value for `flows_in_tbl` is 0.

`nbytes` Total number of bytes that are seen by this `flowacct` action instance, which is 84 in the example. The value includes bytes that are currently in the flow table. The value also includes bytes that have timed out and are no longer in the flow table.

`npackets` Total number of packets that are seen by this `flowacct` action instance, which is 1 in the example. `npackets` includes packets that are currently in the flow table. `npackets` also includes packets that have timed out—are no longer in the flow table.

`usedmem` Memory in bytes in use by the flow table that is maintained by this `flowacct` instance. The `usedmem` value is 256 in the example. The value for `usedmem` is 0 when the flow table does not have any flow records.

IPQoS in Detail (Reference)

This chapter contains reference materials that provide in-depth details about the following IPQoS topics:

- “IPQoS Architecture and the Diffserv Model” on page 757
- “IPQoS Configuration File” on page 770
- “ipqosconf Configuration Utility” on page 774

For an overview, refer to [Chapter 31](#). For planning information, refer to [Chapter 32](#). For procedures for configuring IPQoS, refer to [Chapter 33](#).

IPQoS Architecture and the Diffserv Model

This section describes the IPQoS architecture and how IPQoS implements the differentiated services (Diffserv) model that is defined in RFC 2475, An Architecture for Differentiated Services

(<http://www.ietf.org/rfc/rfc2475.txt?number=2475>). The following elements of the Diffserv model are included in IPQoS:

- Classifier
- Meter
- Marker

In addition, IPQoS includes the flow-accounting module and the `dlcosmk` marker for use with virtual local area network (VLAN) devices.

Classifier Module

In the Diffserv model, the *classifier* is responsible for organizing selected traffic flows into groups on which to apply different service levels. The classifiers that are defined in RFC 2475 were originally designed for boundary routers. In contrast, the IPQoS classifier `ipgpc` is designed to handle traffic flows on hosts that are internal to the local network. Therefore, a network with both IPQoS systems and a Diffserv router can provide a greater degree of differentiated services. For a technical description of `ipgpc`, refer to the `ipgpc(7ipp)` man page.

The `ipgpc` classifier does the following:

1. Selects traffic flows that meet the criteria specified in the IPQoS configuration file on the IPQoS-enabled system
The QoS policy defines various criteria that must be present in packet headers. These criteria are called *selectors*. The `ipgpc` classifier compares these selectors against the headers of packets that are received by the IPQoS system. `ipgpc` then selects all matching packets.
2. Separates the packet flows into *classes*, network traffic with the same characteristics, as defined in the IPQoS configuration file
3. Examines the value in the packet's differentiated service (DS) field for the presence of a differentiated services codepoint (DSCP)
The presence of the DSCP indicates whether the incoming traffic has been marked by the sender with a forwarding behavior.
4. Determines what further action is specified in the IPQoS configuration file for packets of a particular class
5. Passes the packets to the next IPQoS module specified in the IPQoS configuration file, or returns the packets to the network stream

For an overview of the classifier, refer to [“Classifier \(`ipgpc`\) Overview” on page 687](#). For information on invoking the classifier in the IPQoS configuration file, refer to [“IPQoS Configuration File” on page 770](#).

Selectors

The `ipgpc` classifier supports a variety of selectors that you can use in the `filter` clause of the IPQoS configuration file. When you define a filter, always use the minimum number of selectors that are needed to successfully retrieve traffic of a particular class. The number of filters you define can impact IPQoS performance.

The next table lists the selectors that are available for `ipgpc`.

TABLE 36-1 Filter Selectors for the IPQoS Classifier

Selector	Argument	Information Selected
saddr	IP address number.	Source address.
daddr	IP address number.	Destination address.
sport	Either a port number or service name, as defined in <i>/etc/services</i> .	Source port from which a traffic class originated.
dport	Either a port number or service name, as defined in <i>/etc/services</i> .	Destination port to which a traffic class is bound.
protocol	Either a protocol number or protocol name, as defined in <i>/etc/protocols</i> .	Protocol to be used by this traffic class.
dsfield	DS codepoint (DSCP) with a value of 0–63.	DSCP, which defines any forwarding behavior to be applied to the packet. If this parameter is specified, the <code>dsfield_mask</code> parameter must also be specified.
dsfield_mask	Bit mask with a value of 0–255.	Used in tandem with the <code>dsfield</code> selector. <code>dsfield_mask</code> is applied to the <code>dsfield</code> selector to determine which of its bits to match against.
if_name	Interface name.	Interface to be used for either incoming or outgoing traffic of a particular class.
if_groupname	Interface group name.	Interface group to be used for either incoming or outgoing traffic of a particular class.
user	Number of the UNIX user ID or user name to be selected. If no user ID or user name is on the packet, the default <code>-1</code> is used.	User ID that is supplied to an application.
projid	Number of the project ID to be selected.	Project ID that is supplied to an application.
priority	Priority number. Lowest priority is 0.	Priority that is given to packets of this class. Priority is used to order the importance of filters for the same class.
direction	Argument can be one of the following: LOCAL_IN LOCAL_OUT	Direction of packet flow on the IPQoS machine. Input traffic local to the IPQoS system. Output traffic local to the IPQoS system.

TABLE 36-1 Filter Selectors for the IPQoS Classifier (Continued)

Selector	Argument	Information Selected
	FWD_IN	Input traffic to be forwarded.
	FWD_OUT	Output traffic to be forwarded.
precedence	Precedence value. Highest precedence is 0.	Precedence is used to order filters with the same priority.
ip_version	V4 or V6	Addressing scheme that is used by the packets, either IPv4 or IPv6.

Meter Module

The *meter* tracks the transmission rate of flows on a per-packet basis. The meter then determines whether the packet conforms to the configured parameters. The meter module determines the next action for a packet from a set of actions that depend on packet size, configured parameters, and flow rate.

The meter consists of two metering modules, `tokenmt` and `tswtclmt`, which you configure in the IPQoS configuration file. You can configure either module or both modules for a class.

When you configure a metering module, you can define two parameters for rate:

- `committed-rate` – Defines the acceptable transmission rate in bits per second for packets of a particular class
- `peak-rate` – Defines the maximum transmission rate in bits per second that is allowable for packets of a particular class

A metering action on a packet can result in one of three outcomes:

- `green` – The packet causes the flow to remain within its committed rate.
- `yellow` – The packet causes the flow to exceed its committed rate but not its peak rate.
- `red` – The packet causes the flow to exceed its peak rate.

You can configure each outcome with different actions in the IPQoS configuration file. Committed rate and peak rate are explained in the next section.

`tokenmt` Metering Module

The `tokenmt` module uses *token buckets* to measure the transmission rate of a flow. You can configure `tokenmt` to operate as a single-rate or two-rate meter. A `tokenmt` action instance maintains two token buckets that determine whether the traffic flow conforms to configured parameters.

The `tokenmt(7ipp)` man page explains how IPQoS implements the token meter paradigm. You can find more general information about token buckets in Kalevi Kilkki's *Differentiated Services for the Internet* and on a number of web sites.

Configuration parameters for `tokenmt` are as follows:

- `committed_rate` – Specifies the committed rate of the flow in bits per second.
- `committed_burst` – Specifies the committed burst size in bits. The `committed_burst` parameter defines how many outgoing packets of a particular class can pass onto the network at the committed rate.
- `peak_rate` – Specifies the peak rate in bits per second.
- `peak_burst` – Specifies the peak or excess burst size in bits. The `peak_burst` parameter grants to a traffic class a peak-burst size that exceeds the committed rate.
- `color_aware` – Turns on awareness mode for `tokenmt`.
- `color_map` – Defines an integer array that maps DSCP values to green, yellow, or red.

Configuring tokenmt as a Single-Rate Meter

To configure `tokenmt` as a single-rate meter, do not specify a `peak_rate` parameter for `tokenmt` in the IPQoS configuration file. To configure a single-rate `tokenmt` instance to have a red, green, or a yellow outcome, you must specify the `peak_burst` parameter. If you do not use the `peak_burst` parameter, you can configure `tokenmt` to have only a red outcome or green outcome. For an example of a single-rate `tokenmt` with two outcomes, see [Example 33–3](#).

When `tokenmt` operates as a single-rate meter, the `peak_burst` parameter is actually the excess burst size. `committed_rate`, and either `committed_burst` or `peak_burst`, must be nonzero positive integers.

Configuring tokenmt as a Two-Rate Meter

To configure `tokenmt` as a two-rate meter, specify a `peak_rate` parameter for the `tokenmt` action in the IPQoS configuration file. A two-rate `tokenmt` always has the three outcomes, red, yellow, and green. The `committed_rate`, `committed_burst`, and `peak_burst` parameters must be nonzero positive integers.

Configuring tokenmt to Be Color Aware

To configure a two-rate `tokenmt` to be color aware, you must add parameters to specifically add “color awareness.” The following is an example action statement that configures `tokenmt` to be color aware.

EXAMPLE 36–1 Color-Aware `tokenmt` Action for the IPQoS Configuration File

```
action {
  module tokenmt
  name meter1
```

EXAMPLE 36-1 Color-Aware tokenmt Action for the IPQoS Configuration File
(Continued)

```
params {
    committed_rate 4000000
    peak_rate 8000000
    committed_burst 4000000
    peak_burst 8000000
    global_stats true
    red_action_name continue
    yellow_action_name continue
    green_action_name continue
    color_aware true
    color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
}
}
```

You turn on color awareness by setting the `color_aware` parameter to `true`. As a color-aware meter, `tokenmt` assumes that the packet has already been marked as red, yellow, or green by a previous `tokenmt` action. Color-aware `tokenmt` evaluates a packet by using the DSCP in the packet header in addition to the parameters for a two-rate meter.

The `color_map` parameter contains an array into which the DSCP in the packet header is mapped. Consider the following `color_map` array:

```
color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
```

Packets with a DSCP of 0–20 and 22 are mapped to green. Packets with a DSCP of 21 and 23–42 are mapped to red. Packets with a DSCP of 43–63 are mapped to yellow. `tokenmt` maintains a default color map. However, you can change the default as needed by using the `color_map` parameters.

In the `color_action_name` parameters, you can specify `continue` to complete processing of the packet. Or, you can add an argument to send the packet to a marker action, for example, `yellow_action_name mark22`.

`tswtclmt` Metering Module

The `tswtclmt` metering module estimates average bandwidth for a traffic class by using a time-based *rate estimator*. `tswtclmt` always operates as a three-outcome meter. The rate estimator provides an estimate of the flow's arrival rate. This rate should approximate the running average bandwidth of the traffic stream over a specific period or time, its *time window*. The rate estimation algorithm is taken from RFC 2859, *A Time Sliding Window Three Colour Marker*.

You use the following parameters to configure `tswtclmt`:

- `committed_rate` – Specifies the committed rate in bits per second
- `peak_rate` – Specifies the peak rate in bits per second

- `window` – Defines the time window, in milliseconds over which history of average bandwidth is kept

For technical details on `tswtclmt`, refer to the `tswtclmt(7ipp)` man page. For general information on rate shapers that are similar to `tswtclmt`, see RFC 2963, A Rate Adaptive Shaper for Differentiated Services (<http://www.ietf.org/rfc/rfc2963.txt?number=2963>).

Marker Module

IPQoS includes two marker modules, `dscpmk` and `dlcosmk`. This section contains information for using both markers. Normally, you should use `dscpmk` because `dlcosmk` is only available for IPQoS systems with VLAN devices.

For technical information about `dscpmk`, refer to the `dscpmk(7ipp)` man page. For technical information about `dlcosmk`, refer to the `dlcosmk(7ipp)` man page.

Using the `dscpmk` Marker for Forwarding Packets

The marker receives traffic flows after the flows are processed by the classifier or by the metering modules. The marker marks the traffic with a forwarding behavior. This forwarding behavior is the action to be taken on the flows after the flows leaving the IPQoS system. Forwarding behavior to be taken on a traffic class is defined in the *per-hop behavior (PHB)*. The PHB assigns a priority to a traffic class, which indicates the precedence flows of that class in relation to other traffic classes. PHBs only govern forwarding behaviors on the IPQoS system's contiguous network. For more information on PHBs, refer to “Per-Hop Behaviors” on page 692.

Packet forwarding is the process of sending traffic of a particular class to its next destination on a network. For a host such as an IPQoS system, a packet is forwarded from the host to the local network stream. For a Diffserv router, a packet is forwarded from the local network to the router's next hop.

The marker marks the DS field in the packet header with a well-known forwarding behavior that is defined in the IPQoS configuration file. Thereafter, the IPQoS system and subsequent Diffserv-aware systems forward the traffic as indicated in the DS field until the mark changes. To assign a PHB, the IPQoS system marks a value in the DS field of the packet header. This value is called the differentiated services codepoint (DSCP). The Diffserv architecture defines two types of forwarding behaviors, EF and AF, which use different DSCPs. For overview information about DSCPs, refer to “DS Codepoint” on page 691.

The IPQoS system reads the DSCP for the traffic flow and evaluates the flow's precedence in relation to other outgoing traffic flows. The IPQoS system then prioritizes all concurrent traffic flows and releases each flow onto the network by its priority.

The Diffserv router receives the outgoing traffic flows and reads the DS field in the packet headers. The DSCP enables the router to prioritize and schedule the concurrent traffic flows. The router forwards each flow by the priority that is indicated by the PHB. Note that the PHB cannot apply beyond the boundary router of the network unless Diffserv-aware systems on subsequent hops also recognize the same PHB.

Expedited Forwarding (EF) PHB

Expedited forwarding (EF) guarantees that packets with the recommended EF codepoint 46 (101110) receive the best treatment that is available on release to the network. Expedited forwarding is often compared to a leased line. Packets with the 46 (101110) codepoint are guaranteed preferential treatment by all Diffserv routers en route to the packets' destination. For technical information about EF, refer to RFC 2598, *An Expedited Forwarding PHB*.

Assured Forwarding (AF) PHB

Assured forwarding (AF) provides four different classes of forwarding behaviors that you can specify to the marker. The next table shows the classes, the three drop precedences that are provided with each class, and the recommended DSCPs that are associated with each precedence. Each DSCP is represented by its AF value, its value in decimal, and its value in binary.

TABLE 36-2 Assured Forwarding Codepoints

	Class 1	Class 2	Class 3	Class 4
Low-Drop Precedence	AF11 = 10 (001010)	AF21 = 18 (010010)	AF31 = 26 (011010)	AF41 = 34 (100010)
Medium-Drop Precedence	AF12 = 12 (001100)	AF22 = 20 (010100)	AF32 = 28 (011100)	AF42 = 36 (100100)
High-Drop Precedence	AF13 = 14 (001110)	AF23 = 22 (010110)	AF33 = 30 (011110)	AF43 = 38 (100110)

Any Diffserv-aware system can use the AF codepoint as a guide for providing differentiated forwarding behaviors to different classes of traffic.

When these packets reach a Diffserv router, the router evaluates the packets' codepoints along with DSCPs of other traffic in the queue. The router then forwards or drops packets, depending on the available bandwidth and the priorities that are assigned by the packets' DSCPs. Note that packets that are marked with the EF PHB are guaranteed bandwidth over packets that are marked with the various AF PHBs.

Coordinate packet marking between any IPQoS systems on your network and the Diffserv router to ensure that packets are forwarded as expected. For example, suppose IPQoS systems on your network mark packets with AF21 (010010), AF13 (001110), AF43 (100110), and EF (101110) codepoints. You then need to add the AF21, AF13, AF43, and EF DSCPs to the appropriate file on the Diffserv router.

For a technical explanation of the AF codepoint table, refer to RFC 2597. Router manufacturers Cisco Systems and Juniper Networks have detailed information about setting the AF PHB on their web sites. You can use this information to define AF PHBs for IPQoS systems as well as routers. Additionally, router manufacturers' documentation contains instructions for setting DS codepoints on their equipment.

Supplying a DSCP to the Marker

The DSCP is 6 bits in length. The DS field is 1 byte long. When you define a DSCP, the marker marks the first 6 significant bits of the packet header with the DS codepoint. The remaining 2 least-significant bits are unused.

To define a DSCP, you use the following parameter within a marker action statement:

```
dscp_map { 0-63 : DS_codepoint }
```

The `dscp_map` parameter is a 64-element array, which you populate with the (DSCP) value. `dscp_map` is used to map incoming DSCPs to outgoing DSCPs that are applied by the `dscpmk` marker.

You must specify the DSCP value to `dscp_map` in decimal notation. For example, you must translate the EF codepoint of 101110 into the decimal value 46, which results in `dscp_map { 0-63 : 46 }`. For AF codepoints, you must translate the various codepoints that are shown in [Table 36-2](#) to decimal notation for use with `dscp_map`.

Using the `d1cosmk` Marker With VLAN Devices

The `d1cosmk` marker module marks a forwarding behavior in the MAC header of a datagram. You can use `d1cosmk` only on an IPQoS system with a VLAN interface.

`d1cosmk` adds four bytes, which are known as the *VLAN tag*, to the MAC header. The VLAN tag includes a 3-bit user-priority value, which is defined by the IEEE 801.D standard. Diffserv-aware switches that understand VLAN can read the user-priority field in a datagram. The 801.D user priority values implement the class-of-service (CoS) marks, which are well known and understood by commercial switches.

You can use the user-priority values in the `d1cosmk` marker action by defining the class of service marks that are listed in the next table.

TABLE 36-3 801.D User-Priority Values

Class of Service	Definition
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video less than 100ms latency
6	Video less than 10ms latency
7	Network control

For more information on `dlcosmk`, refer to the `dlcosmk(7ipp)` man page.

IPQoS Configuration for Systems With VLAN Devices

This section introduces a simple network scenario that shows how to implement IPQoS on systems with VLAN devices. The scenario includes two IPQoS systems, `machine1` and `machine2`, that are connected by a switch. The VLAN device on `machine1` has the IP address `10.10.8.1`. The VLAN device on `machine2` has the IP address `10.10.8.3`.

The following IPQoS configuration file for `machine1` shows a simple solution for marking traffic through the switch to `machine2`.

EXAMPLE 36-2 IPQoS Configuration File for a System With a VLAN Device

```
fmt_version 1.0
action {
    module ipgpc
        name ipgpc.classify

    filter {
        name myfilter2
        daddr 10.10.8.3
        class myclass
    }

    class {
        name myclass
        next_action mark4
    }
}

action {
```

EXAMPLE 36–2 IPQoS Configuration File for a System With a VLAN Device (Continued)

```
name mark4
module dlcosmk
params {
    cos 4
    next_action continue
global_stats true
}
}
```

In this configuration, all traffic from `machine1` that is destined for the VLAN device on `machine2` is passed to the `dlcosmk` marker. The `mark4` marker action instructs `dlcosmk` to add a VLAN mark to datagrams of class `myclass` with a CoS of 4. The user-priority value of 4 indicates that the switch between the two machines should give controlled load forwarding to `myclass` traffic flows from `machine1`.

flowacct Module

The IPQoS `flowacct` module records information about traffic flows, a process that is referred to as *flow accounting*. Flow accounting produces data that can be used for billing customers or for evaluating the amount of traffic to a particular class.

Flow accounting is optional. `flowacct` is typically the final module that metered or marked traffic flows might encounter before release onto the network stream. For an illustration of `flowacct`'s position in the Diffserv model, see [Figure 31–1](#). For detailed technical information about `flowacct`, refer to the `flowacct(7ipp)` man page.

To enable flow accounting, you need to use the Solaris `exacct` accounting facility and the `acctadm` command, as well as `flowacct`. For the overall steps in setting up flow accounting, refer to “[Setting Up Flow Accounting \(Task Map\)](#)” on page 751.

flowacct Parameters

The `flowacct` module gathers information about flows in a *flow table* that is composed of *flow records*. Each entry in the table contains one flow record. You cannot display a flow table.

In the IPQoS configuration file, you define the following `flowacct` parameters to measure flow records and to write the records to the flow table:

- `timer` – Defines an interval, in milliseconds, when timed-out flows are removed from the flow table and written to the file that is created by `acctadm`
- `timeout` – Defines an interval, in milliseconds, which specifies how long a packet flow must be inactive before the flow times out

Note – You can configure `timer` and `timeout` to have different values.

- `max_limit` – Places an upper limit on the number of flow records that can be stored in the flow table

For an example of how `flowacct` parameters are used in the IPQoS configuration file, refer to [“How to Configure Flow Control in the IPQoS Configuration File”](#) on page 737.

Flow Table

The `flowacct` module maintains a flow table that records all packet flows that are seen by a `flowacct` instance. A flow is identified by the following parameters, which include the `flowacct` 8-tuple:

- Source address
- Destination address
- Source port
- Destination port
- DSCP
- User ID
- Project ID
- Protocol Number

If all the parameters of the 8-tuple for a flow remain the same, the flow table contains only one entry. The `max_limit` parameter determines the number of entries that a flow table can contain.

The flow table is scanned at the interval that is specified in the IPQoS configuration file for the `timer` parameter. The default is 15 seconds. A flow “times out” when its packets are not seen by the IPQoS system for at least the `timeout` interval in the IPQoS configuration file. The default timeout interval is 60 seconds. Entries that have timed out are then written to the accounting file that is created with the `acctadm` command.

flowacct Records

A `flowacct` record contains the attributes described in the following table.

TABLE 36-4 Attributes of a `flowacct` Record

Attribute Name	Attribute Contents	Type
<code>src-addr-address-type</code>	Source address of the originator. <i>address-type</i> is either v4 for IPv4 or v6 for IPv6, as specified in the IPQoS configuration file.	Basic
<code>dest-addr-address-type</code>	Destination address for the packets. <i>address-type</i> is either v4 for IPv4 or v6 for IPv6, as specified in the IPQoS configuration file.	Basic
<code>src-port</code>	Source port from which the flow originated.	Basic
<code>dest-port</code>	Destination port number to which this flow is bound.	Basic
<code>protocol</code>	Protocol number for the flow.	Basic
<code>total-packets</code>	Number of packets in the flow.	Basic
<code>total-bytes</code>	Number of bytes in the flow.	Basic
<code>action-name</code>	Name of the <code>flowacct</code> action that recorded this flow.	Basic
<code>creation-time</code>	First time that a packet is seen for the flow by <code>flowacct</code> .	Extended only
<code>last-seen</code>	Last time that a packet of the flow was seen.	Extended only
<code>diffserv-field</code>	DSCP in the outgoing packet headers of the flow.	Extended only
<code>user</code>	Either a UNIX User ID or user name, which is obtained from the application.	Extended only
<code>projid</code>	Project ID, which is obtained from the application.	Extended only

Using `acctadm` with the `flowacct` Module

You use the `acctadm` command to create a file in which to store the various flow records that are generated by `flowacct`. `acctadm` works in conjunction with the extended accounting facility. For technical information about `acctadm`, refer to the `acctadm(1M)` man page.

The `flowacct` module observes flows and fills the flow table with flow records. `flowacct` then evaluates its parameters and attributes in the interval that is specified by `timer`. When a packet is not seen for at least the `last_seen` plus `timeout` values, the packet times out. All timed-out entries are deleted from the flow table. These entries are then written to the accounting file each time the interval that is specified in the `timer` parameter elapses.

To invoke `acctadm` for use with the `flowacct` module, use the following syntax:

```
acctadm -e file-type -f filename flow
```

`acctadm -e` Invokes `acctadm` with the `-e` option. The `-e` indicates that a resource list follows.

file-type Specifies the attributes to be gathered. *file-type* must be replaced by either `basic` or `extended`. For a list of attributes in each file type, refer to [Table 36-4](#).

`-f file-name` Creates the file *file-name* to hold the flow records.

`flow` Indicates that `acctadm` is to be run with IPQoS.

IPQoS Configuration File

This section contains full details about the parts of the IPQoS configuration file. The IPQoS boot-time activated policy is stored in the file `/etc/inet/ipqosinit.conf`. Although you can edit this file, the best practice for a new IPQoS system is to create a configuration file with a different name. Tasks for applying and debugging an IPQoS configuration are in [Chapter 33](#).

The syntax of the IPQoS configuration file is shown in [Example 36-3](#). The example uses the following conventions:

- **computer-style type** – Syntactical information that is provided to explain the parts of the configuration file. You do not type any text that appears in computer-style type.
- **bold type** – Literal text that you must type in the IPQoS configuration file. For example, you must always begin the IPQoS configuration file with **`fmt_version`**.
- *italic type* – Variable text that you replace with descriptive information about your configuration. For example, you must always replace *action-name* or *module-name* with information that pertains to your configuration.

EXAMPLE 36-3 Syntax of the IPQoS Configuration File

```
file_format_version ::= fmt_version version

action_clause ::= action {
    name action-name
    module module-name
    params-clause | ""
    cf-clauses
}
action_name ::= string
module_name ::= ipgpc | dlcosmk | dscpmk | tswtclmt | tokenmt | flowacct
```

EXAMPLE 36-3 Syntax of the IPQoS Configuration File (Continued)

```
params_clause ::= params {
    parameters
    params-stats | ""
}
parameters ::= prm-name-value parameters | ""
prm_name_value ::= param-name param-value

params_stats ::= global-stats boolean

cf_clauses ::= class-clause cf-clauses |
             filter-clause cf-clauses | ""

class_clause ::= class {
    name class-name
    next_action next-action-name
    class-stats | ""
}
class_name ::= string
next_action_name ::= string
class_stats ::= enable_stats boolean
boolean ::= TRUE | FALSE

filter_clause ::= filter {
    name filter-name
    class class-name
    parameters
}
filter_name ::= string
```

The remaining text describes each major part of the IPQoS configuration file.

action Statement

You use `action` statements to invoke the various IPQoS modules that are described in [“IPQoS Architecture and the Diffserv Model”](#) on page 757.

When you create the IPQoS configuration file, you must always begin with the version number. Then, you must add the following `action` statement to invoke the classifier:

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
}
```

Follow the classifier `action` statement with a `params` clause or a `class` clause.

Use the following syntax for all other `action` statements:

```
action {  
  name action-name  
  module module-name  
  params-clause | ""  
  cf-clauses  
}
```

<code>name <i>action_name</i></code>	Assigns a name to the action.
<code>module <i>module_name</i></code>	Identifies the IPQoS module to be invoked, which must be one of the modules in Table 36-5 .
<code><i>params_clause</i></code>	Can be parameters for the classifier to process, such as global statistics or the next action to process.
<code><i>cf_clauses</i></code>	A set of zero or more <code>class</code> clauses or <code>filter</code> clauses

Module Definitions

The module definition indicates which module is to process the parameters in the `action` statement. The IPQoS configuration file can include the following modules.

TABLE 36-5 IPQoS Modules

Module Name	Definition
<code>ipgpc</code>	IP classifier
<code>dscpmk</code>	Marker to be used to create DSCPs in IP packets
<code>dlcosmk</code>	Marker to be used with VLAN devices
<code>tokenmt</code>	Token bucket meter
<code>tswtclmt</code>	Time-sliding window meter
<code>flowacct</code>	Flow-accounting module

class Clause

You define a `class` clause for each class of traffic.

Use this syntax to define the remaining classes in the IPQoS configuration:

```
class {
    name class-name
    next_action next-action-name
}
```

To enable statistics collection on a particular class, you must first enable global statistics in the `ipgpc.classify` action statement. For more information, refer to “[action Statement](#)” on page 771.

Use the `enable_stats TRUE` statement whenever you want to turn on statistics collection for a class. If you do not need to gather statistics for a class, you can specify `enable_stats FALSE`. Alternatively, you can eliminate the `enable_stats` statement.

Traffic on an IPQoS-enabled network that you do not specifically define is relegated to the *default class*.

filter Clause

Filters are made up of selectors that group traffic flows into classes. These selectors specifically define the criteria to be applied to traffic of the class that was created in the class clause. If a packet matches all selectors of the highest-priority filter, the packet is considered to be a member of the filter’s class. For a complete list of selectors that you can use with the `ipgpc` classifier, refer to [Table 36–1](#).

You define filters in the IPQoS configuration file by using a *filter clause*, which has the following syntax:

```
filter {
    name filter-name
    class class-name
    parameters (selectors)
}
```

params Clause

The `params` clause contains processing instructions for the module that is defined in the action statement. Use the following syntax for the `params` clause:

```
params {
    parameters
    params-stats | ""
}
```

In the `params` clause, you use parameters that are applicable to the module.

The *params-stats* value in the *params* clause is either `global_stats TRUE` or `global_stats FALSE`. The `global_stats TRUE` instruction turns on UNIX style statistics for the `action` statement where global statistics is invoked. You can view the statistics by using the `kstat` command. You must enable `action` statement statistics before you can enable per-class statistics.

ipqosconf Configuration Utility

You use the `ipqosconf` utility to read the IPQoS configuration file and to configure IPQoS modules in the UNIX kernel. `ipqosconf` performs the following actions:

- Applies the configuration file to the IPQoS kernel modules (`ipqosconf -a filename`)
- Lists the IPQoS configuration file currently resident in the kernel (`ipqosconf -l`)
- Ensures that the current IPQoS configuration is read and applied each time the machine reboots (`ipqosconf -c`)
- Flushes the current IPQoS kernel modules (`ipqosconf -f`)

For technical information, refer to the `ipqosconf(1M)` man page.

Glossary

This glossary contains definitions of new terms in this book that are not in the *Sun Global Glossary* available from the `docs.sun.com` web site.

3DES	See Triple-DES .
address pool	In Mobile IP, a set of addresses that are designated by the home network administrator for use by mobile nodes that need a home address.
AES	Advanced Encryption Standard. A symmetric 128-bit block data encryption technique. The U.S. government adopted the Rijndael variant of the algorithm as its encryption standard in October 2000. AES replaces DES encryption as the government standard.
agent advertisement	In Mobile IP, a message that is periodically sent by home agents and foreign agents to advertise their presence on any attached link.
agent discovery	In Mobile IP, the process by which a mobile node determines if it has moved, its current location, and its care-of address on a foreign network.
anycast address	An IPv6 address that is assigned to a group of interfaces (typically belonging to different nodes). A packet that is sent to an anycast address is routed to the <i>nearest</i> interface having that address. The packet's route is in compliance with the routing protocol's measure of distance.
anycast group	A group of interfaces with the same anycast IPv6 address. The Solaris OS implementation of IPv6 does not support the creation of anycast addresses and groups. However, Solaris IPv6 nodes can send traffic to anycast groups.

asymmetric key cryptography	An encryption system in which the sender and receiver of a message use different keys to encrypt and decrypt the message. Asymmetric keys are used to establish a secure channel for symmetric key encryption. The Diffie-Hellman protocol is an example of an asymmetric key protocol. Contrast with symmetric key cryptography .
authentication header	An extension header that provides authentication and integrity, without confidentiality, to IP datagrams.
autoconfiguration	The process where a host automatically configures its IPv6 address from the site prefix and the local MAC address.
bidirectional tunnel	A tunnel that can transmit datagrams in both directions.
binding table	In Mobile IP, a home agent table that associates a home address with a care-of address, including remaining lifetime and time granted.
Blowfish	A symmetric block cipher algorithm that takes a variable-length key from 32 bits to 448 bits. Its author, Bruce Schneier, claims that Blowfish is optimized for applications where the key does not change often.
broadcast address	IPv4 network addresses with the host portion of the address having all zeroes (10.50.0.0) or all one bits (10.50.255.255). A packet that is sent to a broadcast address from a machine on the local network is delivered to all machines on that network.
CA	See certificate authority (CA) .
care-of address	A mobile node's temporary address that is used as a tunnel exit point when the mobile node is connected to a foreign network.
certificate authority (CA)	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The CA guarantees the identity of the individual who is granted the unique certificate.
certificate revocation list (CRL)	A list of public key certificates that have been revoked by a CA.
classless inter-domain routing (CIDR) address	An IPv4 address format that is not based on network classes (Class A, B, and C). CIDR addresses are 32 bits in length. They use the standard IPv4 dotted decimal notation format, with the addition of a network prefix. This prefix defines the network number and the network mask.
class	In IPQoS, a group of network flows that share similar characteristics. You define classes in the IPQoS configuration file.
datagram	See IP datagram .
DES	Data Encryption Standard. A symmetric-key encryption method developed in 1975 and standardized by ANSI in 1981 as ANSI X.3.92. DES uses a 56-bit key.

diffserv model	Internet Engineering Task Force architectural standard for implementing differentiated services on IP networks. The major modules are classifier, meter, marker, scheduler, and dropper. IPQoS implements the classifier, meter, and marker modules. The diffserv model is described in RFC 2475, <i>An Architecture for Differentiated Services</i> .
digital signature	A digital code that is attached to an electronically transmitted message that uniquely identifies the sender.
domain of interpretation (DOI)	A DOI defines data formats, network traffic exchange types, and conventions for naming security-relevant information. Security policies, cryptographic algorithms, and cryptographic modes are examples of security-relevant information.
DSA	Digital Signature Algorithm. A public key algorithm with a variable key size from 512 to 4096 bits. The U.S. Government standard, DSS, goes up to 1024 bits. DSA relies on SHA-1 for input.
DS codepoint (DSCP)	A 6-bit value that, when included in the DS field of an IP header, indicates how a packet must be forwarded.
Diffie-Hellman protocol	Also known as public key cryptography. An asymmetric cryptographic key agreement protocol that was developed by Diffie and Hellman in 1976. The protocol enables two users to exchange a secret key over an insecure medium without any prior secrets. Diffie-Hellman is used by the IKE protocol.
dual stack	A TCP/IP protocol stack with both IPv4 and IPv6 at the network layer, with the rest of the stack being identical. When you enable IPv6 during Solaris OS installation, the host receives the dual-stack version of TCP/IP.
dynamic packet filter	See stateful packet filter .
encapsulating security payload (ESP)	An extension header that provides integrity and confidentiality to datagrams.
encapsulation	The process of a header and payload being placed in the first packet, which is subsequently placed in the second packet's payload.
failback	The process of switching back network access to an interface that has its repair detected.
failover	The process of switching network access from a failed interface to a good physical interface. Network access includes IPv4 unicast, multicast, and broadcast traffic, as well as IPv6 unicast and multicast traffic.
failure detection	The process of detecting when an interface or the path from an interface to an Internet layer device no longer works. IP network multipathing (IPMP) includes two types of failure detection: link based (default) and probe based (optional).

filter	A set of rules that define the characteristics of a class in the IPQoS configuration file. The IPQoS system selects for processing any traffic flows that conform to the filters in its IPQoS configuration file. See packet filter .
firewall	Any device or software that isolates an organization's private network or intranet from the Internet, thus protecting it from external intrusions. A firewall can include packet filtering, proxy servers, and NAT (network address translation).
flow accounting	In IPQoS, the process of accumulating and recording information about traffic flows. You establish flow accounting by defining parameters for the <code>flowacct</code> module in the IPQoS configuration file.
foreign agent	A router or server on the foreign network that the mobile node visits.
foreign network	Any network other than the mobile node's home network.
forward tunnel	A tunnel that starts at the home agent and terminates at the mobile node's care-of address.
Generic Routing Encapsulation (GRE)	An optional form of tunneling that can be supported by home agents, foreign agents, and mobile nodes. GRE enables a packet of any network-layer protocol to be encapsulated within a delivery packet of any other (or the same) network-layer protocol.
hash value	A number that is generated from a string of text. Hash functions are used to ensure that transmitted messages have not been tampered with. MD5 and SHA-1 are examples of one-way hash functions.
header	See IP header .
HMAC	Keyed hashing method for message authentication. HMAC is a secret key authentication algorithm. HMAC is used with an iterative cryptographic hash function, such as MD5 or SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.
home address	An IP address that is assigned for an extended period to a mobile node. The address remains unchanged when the node is attached elsewhere on the Internet or an organization's network.
home agent	A router or server on the home network of a mobile node.
home network	A network that has a network prefix that matches the network prefix of a mobile node's home address.
hop	A measure that is used to identify the number of routers that separate two hosts. If three routers separate a source and destination, the hosts are four hops away from each other.

host	A system that does not perform packet forwarding. Upon installation of the Solaris OS, a system becomes a host by default, that is, the system cannot forward packets. A host typically has one physical interface, although it can have multiple interfaces.
ICMP	Internet Control Message Protocol. Used to handle errors and exchange control messages.
ICMP echo request packet	A packet sent to a machine on the Internet to solicit a response. Such packets are commonly known as “ping” packets.
IKE	Internet Key Exchange. IKE automates the provision of authenticated keying material for IPsec security association (SA) s.
Internet Protocol (IP)	The method or protocol by which data is sent from one computer to another on the Internet.
IP	See Internet Protocol (IP) , IPv4 , IPv6 .
IP datagram	A packet of information that is carried over IP. An IP datagram contains a header and data. The header includes the addresses of the source and the destination of the datagram. Other fields in the header help identify and recombine the data with accompanying datagrams at the destination.
IP header	Twenty bytes of data that uniquely identify an Internet packet. The header includes source and destination addresses for the packet. An option exists within the header to allow further bytes to be added.
IP in IP encapsulation	The mechanism for tunneling IP packets within IP packets.
IP link	A communication facility or medium over which nodes can communicate at the link layer. The link layer is the layer immediately below IPv4/IPv6. Examples include Ethernets (simple or bridged) or ATM networks. One or more IPv4 subnet numbers or prefixes are assigned to an IP link. A subnet number or prefix cannot be assigned to more than one IP link. In ATM LANE, an IP link is a single emulated LAN. When you use ARP, the scope of the ARP protocol is a single IP link.
IPQoS	A software feature that provides an implementation of the diffserv model standard, plus flow accounting and 802.1 D marking for virtual LANs. Using IPQoS, you can provide different levels of network services to customers and applications, as defined in the IPQoS configuration file.
IPsec	IP security. The security architecture that provides protection for IP datagrams.
IP stack	TCP/IP is frequently referred to as a “stack.” This refers to the layers (TCP, IP, and sometimes others) through which all data passes at both client and server ends of a data exchange.

IPv4	Internet Protocol, version 4. IPv4 is sometimes referred to as IP. This version supports a 32-bit address space.
IPv6	Internet Protocol, version 6. IPv6 supports a 128-bit address space.
key management	The way in which you manage security association (SA) s.
keystore name	The name that an administrator gives to the storage area, or keystore, on a network interface card (NIC) . The keystore name is also called the token or the token ID.
link-local address	In IPv6, a designation that is used for addressing on a single link for purposes such as automatic address configuration. By default, the link-local address is created from the system's MAC address.
local-use address	A unicast address that has only local routability scope (within the subnet or within a subscriber network). This address also can have a local or global uniqueness scope.
link layer	The layer immediately below IPv4/IPv6 .
marker	<ol style="list-style-type: none"> 1. A module in the diffserv architecture and IPQoS that marks the DS field of an IP packet with a value that indicates how the packet is to be forwarded. In the IPQoS implementation, the marker module is <code>dscpmk</code>. 2. A module in the IPQoS implementation that marks the virtual LAN tag of an Ethernet datagram with a user priority value. The user priority value indicates how datagrams are to be forwarded on a network with VLAN devices. This module is called <code>dlcosmk</code>.
MD5	An iterative cryptographic hash function that is used for message authentication, including digital signatures. The function was developed in 1991 by Rivest.
message authentication code (MAC)	MAC provides assurance of data integrity and authenticates data origin. MAC does not protect against eavesdropping.
meter	A module in the diffserv architecture that measures the rate of traffic flow for a particular class. The IPQoS implementation includes two meters, <code>tokenmt</code> and <code>tswtc1mt</code> .
Minimal encapsulation	An optional form of IPv4 in IPv4 tunneling that can be supported by home agents, foreign agents, and mobile nodes. Minimal encapsulation has 8 or 12 bytes less of overhead than does IP in IP encapsulation.
mobile node	A host or router that can change its point of attachment from one network to another network while maintaining all existing communications by using its IP home address.
mobility agent	Either a home agent or a foreign agent.

mobility binding	The association of a home address with a care-of address, along with the remaining lifetime of that association.
mobility security association	A collection of security measures, such as an authentication algorithm, between a pair of nodes, which are applied to Mobile IP protocol messages that are exchanged between the two nodes.
MTU	Maximum Transmission Unit. The size, given in octets, that can be transmitted over a link. For example, the MTU of an Ethernet is 1500 octets.
multicast address	An IPv6 address that identifies a group of interfaces in a particular way. A packet that is sent to a multicast address is delivered to all of the interfaces in the group. The IPv6 multicast address has similar functionality to the IPv4 broadcast address.
multihomed host	A system that has more than one physical interface and that does not perform packet forwarding. A multihomed host can run routing protocols.
NAT	See network address translation .
neighbor advertisement	A response to a neighbor solicitation message or the process of a node sending unsolicited neighbor advertisements to announce a link-layer address change.
neighbor discovery	An IP mechanism that enables hosts to locate other hosts that reside on an attached link.
neighbor solicitation	A solicitation that is sent by a node to determine the link-layer address of a neighbor. A neighbor solicitation also verifies that a neighbor is still reachable by a cached link-layer address.
Network Access Identifier (NAI)	A designation that uniquely identifies the mobile node in the format of user@domain.
network address translation	NAT. The translation of an IP address used within one network to a different IP address known within another network. Used to limit the number of global IP addresses that are needed.
network interface card (NIC)	Network adapter that is either internal or a separate card that serves as an interface to a link. Some NICs can have multiple physical interfaces, such as the qfe card. The Sun Crypto Accelerator 4000 board is a NIC.
node	In IPv6, any system that is IPv6-enabled, whether a host or a router.
outcome	The action to take as a result of metering traffic. The IPQoS meters have three outcomes, red, yellow, and green, which you define in the IPQoS configuration file.
packet	A group of information that is transmitted as a unit over communications lines. Contains an IP header plus a payload .

packet filter	A firewall function that can be configured to allow or disallow specified packets through a firewall.
packet header	See IP header .
payload	The data that is carried in a packet. The payload does not include the header information that is required to get the packet to its destination.
perfect forward secrecy (PFS)	In PFS, the key that is used to protect transmission of data is not used to derive additional keys. Also, the source of the key that is used to protect data transmission is never used to derive additional keys. PFS applies to authenticated key exchange only. See also Diffie-Hellman protocol .
per-hop behavior (PHB)	A priority that is assigned to a traffic class. The PHB indicates the precedence which flows of that class have in relation to other traffic classes.
physical interface	A system's attachment to a link. This attachment is often implemented as a device driver plus a network interface card (NIC). Some NICs can have multiple points of attachment, for example, <code>qfe</code> .
physical interface group	The set of physical interfaces on a system that are connected to the same link. These interfaces are identified by assigning the same (non-null) character string name to all the physical interfaces in the group.
physical interface group name	A name that is assigned to a physical interface that identifies the group. The name is local to a system. Multiple physical interfaces, sharing the same group name, form a physical interface group.
PKI	Public Key Infrastructure. A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.
private address	An IP address that is not routable through the Internet. Private addresses can be used by internal networks on hosts that do not require Internet connectivity. These addresses are defined in Address Allocation for Private Internets (http://www.ietf.org/rfc/rfc1918.txt?number=1918) and often referred to as "1918" addresses.
protocol stack	See IP stack .
proxy server	A server that sits between a client application, such as a Web browser, and another server. Used to filter requests—to prevent access to certain web sites, for instance.
public key cryptography	A cryptographic system that uses two different keys. The public key is known to everyone. The private key is known only to the recipient of the message. IKE provides public keys for IPsec.

redirect	In a router, to inform a host of a better first-hop node to reach a particular destination.
registration	The process by which a mobile node registers its care-of address with its home agent and foreign agent when it is away from home.
repair detection	The process of detecting when a NIC or the path from the NIC to some layer-3 device starts operating correctly after a failure.
replay attack	In IPsec, an attack in which a packet is captured by an intruder. The stored packet then replaces or repeats the original at a later time. To protect against such attacks, a packet can contain a field that increments during the lifetime of the secret key that is protecting the packet.
reverse tunnel	A tunnel that starts at the mobile node's care-of address and terminates at the home agent.
router	A system that usually has more than one interface, runs routing protocols, and forwards packets. You can configure a system with only one interface as a router if the system is the endpoint of a PPP link.
router advertisement	The process of routers advertising their presence together with various link and Internet parameters, either periodically or in response to a router solicitation message.
router discovery	The process of hosts locating routers that reside on an attached link.
router solicitation	The process of hosts requesting routers to generate router advertisements immediately, rather than at their next scheduled time.
RSA	A method for obtaining digital signatures and public key cryptosystems. The method was first described in 1978 by its developers, Rivest, Shamir, and Adleman.
SA	See security association (SA) .
SADB	Security Associations Database. A table that specifies cryptographic keys and cryptographic algorithms. The keys and algorithms are used in the secure transmission of data.
SCTP	See streams control transport protocol .
security association (SA)	An association that specifies security properties from one host to a second host.
security parameter index (SPI)	An integer that specifies the row in the security associations database (SADB) that a receiver should use to decrypt a received packet.
security policy database (SPD)	Database that specifies the level of protection to apply to a packet. The SPD filters IP traffic to determine whether a packet should be discarded, should be passed in the clear, or should be protected with IPsec.

selector	The element that specifically defines the criteria to be applied to packets of a particular class in order to select that traffic from the network stream. You define selectors in the filter clause of the IPQoS configuration file.
SHA-1	Secure Hashing Algorithm. The algorithm operates on any input length less than 2^{64} to produce a message digest. The SHA-1 algorithm is input to DSA.
site-local-use address	A designation that is used for addressing on a single site.
smurf attack	To use ICMP echo request packets directed to an IP broadcast address or multiple broadcast addresses from remote locations to create severe network congestion or outages.
sniff	To eavesdrop on computer networks—frequently used as part of automated programs to sift information, such as clear-text passwords, off the wire.
spoof	To gain unauthorized access to a computer by sending a message to it with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.
SPD	See security policy database (SPD) .
SPI	See security parameter index (SPI) .
stack	See IP stack .
standby	A physical interface that is not used to carry data traffic unless some other physical interface has failed.
stateful packet filter	A packet filter that can monitor the state of active connections and use the information obtained to determine which network packets to allow through the firewall . By tracking and matching requests and replies, a stateful packet filter can screen for a reply that doesn't match a request.
stateless autoconfiguration	The process of a host generating its own IPv6 addresses by combining its MAC address and an IPv6 prefix that is advertised by a local IPv6 router.
stream control transport protocol	A transport layer protocol that provides connection-oriented communications in a manner similar to TCP. Additionally, SCTP supports multi-homing, in which one of the endpoints of the connection can have more than one IP address.

symmetric key cryptography	An encryption system in which the sender and receiver of a message share a single, common key. This common key is used to encrypt and decrypt the message. Symmetric keys are used to encrypt the bulk of data transmission in IPsec. DES is one example of a symmetric key system.
TCP/IP	TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).
Triple-DES	Triple-Data Encryption Standard. A symmetric-key encryption method. Triple-DES requires a key length of 168 bits. Triple-DES is also written as 3DES.
tunnel	The path that is followed by a datagram while it is encapsulated. See encapsulation .
unicast address	An IPv6 address that identifies a single interface of an IPv6-enabled node. The parts of the unicast address are site prefix, subnet ID, and interface ID.
user-priority	A 3-bit value that implements class-of-service marks, which define how Ethernet datagrams are forwarded on a network of VLAN devices.
virtual LAN (VLAN) device	Network interfaces that provide traffic forwarding at the Ethernet (data link) level of the IP protocol stack.
virtual private network (VPN)	A single, secure, logical network that uses tunnels across a public network such as the Internet.
visited network	A network other than a mobile node's home network, to which the mobile node is currently connected.
visitor list	The list of mobile nodes that are visiting a foreign agent.

Index

Numbers and Symbols

- * (asterisk), wildcard in bootparams database, 198
- > prompt
 - ikeadm command mode, 493
 - ipseckey command mode, 462
- “r” commands, in UNIX, 41
- 3DES encryption algorithm
 - IPsec and, 434
 - key length, 463
- 6to4 address
 - format, 206
 - host address, 207
- 6to4 advertisement, 135
- 6to4 prefix
 - /etc/inet/ndpd.conf advertisement, 135
 - explanation of parts, 206
- 6to4 pseudo-interface configuration, 134
- 6to4 relay router
 - in a 6to4 tunnel, 218
 - security issues, 180, 239-241
 - tunnel configuration tasks, 136, 137
 - tunnel topology, 240
- 6to4 router configuration
 - examples, 135
 - tasks, 134
- 6to4 tunnel, 237-241
 - 6to4 relay router, 136
 - definition, 133
 - known problems, 180
 - packet flow, 239, 240
 - sample topology, 238

- 6to4relay command, 137
 - definition, 218
 - examples, 218
 - syntax, 218
 - tunnel configuration tasks, 137

A

- a option
 - ikecert certdb command, 499, 502
 - ikecert certrldb command, 512
 - ikecert command, 506
 - ipseconf command, 447, 493
- A option
 - ikecert certlocal command, 497
 - ikecert command, 531
- AAAA records, 140, 242
- accelerating
 - IKE computations, 481, 521-522
- acctadm command, for flow accounting, 689, 754, 769
- ACK segment, 45
- action statement, 771
- active-active interface configuration, IPMP, 645
- active rule sets, *See* Solaris IP Filter
- active-standby interface configuration, IPMP, 645
- adding
 - CA certificates (IKE), 501-506
 - IPsec SAs, 446, 461-465
 - keys manually (IPsec), 461-465
 - preshared keys (IKE), 491-494

- adding (Continued)
 - public key certificates (IKE), 501-506
 - self-signed certificates (IKE), 497
- address autoconfiguration
 - definition, 81, 82-83
 - enabling, on an IPv6 node, 142
 - IPv6, 222, 227
- address pools
 - appending, 564-565
 - configuring, 541-542
 - overview, 541-542
 - removing, 564
 - viewing, 563-564
 - viewing statistics, 568
- address resolution, in IPv6, 81
- Address Resolution Protocol (ARP)
 - comparison to Neighbor Discovery protocol, 230-232
 - definition, 39
- Address section
 - labels and values, 626
 - Mobile IP configuration file, 624, 626-630
 - NAI labels and values, 628
 - Node-Default labels and values, 629
 - private addresses, 626, 627
- addresses
 - 6to4 format, 206
 - CIDR format, 58
 - data addresses, IPMP, 642
 - default address selection, 173-176
 - displaying addresses of all
 - interfaces, 155-156
 - Ethernet addresses
 - ethers database, 194, 198
 - IPv4 format, 57
 - IPv4 netmask, 189
 - IPv6, 6to4 format, 134
 - IPv6 global unicast, 77-78
 - IPv6 link-local, 79
 - loopback address, 186
 - multicast, in IPv6, 207-208
 - temporary, in IPv6, 144-147
 - test addresses, IPMP, 642-643
- administrative subdivisions, 64
- Advertisements section
 - labels and values, 622
 - Mobile IP configuration file, 621-623
- AdvertiseOnBcast label, 602, 622
- AdvFrequency label, 602, 622
- AdvInitCount label, 623
- AdvLifetime label, 602, 607, 622
- AdvLimitUnsolicited label, 623
- AES encryption algorithm, IPsec and, 434
- agent advertisement
 - Mobile IP, 587
 - over dynamic interfaces, 587, 621
- agent discovery, Mobile IP, 587-588
- agent solicitation, Mobile IP, 586, 587, 588
- AH, *See* authentication header (AH)
- anonymous FTP program, description, 41
- anonymous login name, 41
- anycast addresses, 137
 - definition, 80
- anycast groups, 6to4 relay router, 137
- application layer
 - OSI, 36
 - packet life cycle
 - receiving host, 47
 - sending host, 44
 - TCP/IP, 40, 42
 - description, 37, 40
 - file services, 42
 - name services, 41
 - network administration, 42
 - routing protocols, 42
 - standard TCP/IP services, 40, 41
 - UNIX "r" commands, 41
- application server, configuring for IPQoS, 731
- assured forwarding (AF), 692, 764
 - AF codepoints table, 764
 - for a marker action statement, 725
- asterisk (*), wildcard in bootparams
 - database, 198
- ATM, IPMP support for, 657
- ATM support, IPv6 over, 244
- auth_algs security option, ifconfig
 - command, 474-475
- authentication algorithms
 - IKE, 531
 - specifying for IPsec, 474
- authentication header (AH)
 - IPsec protection mechanism, 432-434
 - protecting IP datagram, 432
 - protecting IP packets, 425
 - security considerations, 433
- automatic tunnels, transition to IPv6, 234

B

- bandwidth regulation, 685
 - planning, in the QoS policy, 703
- BaseAddress label, 603, 625
- binary to decimal conversion, 190
- binding table
 - home agent, 612, 614
 - Mobile IP, 631
- Blowfish encryption algorithm, IPsec and, 434
- booting, network configuration server booting protocols, 98
- BOOTP protocol
 - and DHCP, 247
 - supporting clients with DHCP service, 321
- BOOTP relay agent
 - configuring
 - with DHCP Manager, 283
 - with `dhcpconfig -R`, 288
 - hops, 309
- bootparams database
 - corresponding name service files, 194
 - overview, 197
 - wildcard entry, 198
- Bootparams protocol, 98
- boundary router, in 6to4 site, 238
- broadcast address, 625
- broadcast datagrams, Mobile IP, 596
- BSD-based operating systems
 - `/etc/inet/hosts` file link, 185
 - `/etc/inet/netmasks` file link, 191
- bypassing
 - IPsec on LAN, 456
 - IPsec policy, 435

C

- `-c` option, in `.iked` daemon, 488
- care-of address
 - acquiring, 588
 - colocated, 586, 588, 593, 596
 - foreign agent, 588, 591, 594
 - Mobile IP, 582
 - mobile node location, 584
 - mobile node registration, 591
 - mobility agents, 583
 - sharing, 588
 - state information, 632

- `cert_root` keyword
 - IKE configuration file, 503, 508
- `cert_trust` keyword
 - IKE configuration file, 499, 508
 - `ikecert` command and, 531
- certificate requests
 - from CA, 501
 - on hardware, 507
 - use, 531
- certificate revocation lists, *See* CRLs
- certificates
 - adding to database, 502
 - creating self-signed (IKE), 497
 - description, 502
 - from CA, 502
 - from CA on hardware, 509
 - ignoring CRLs, 504
 - IKE, 480
 - in `ike/config` file, 508
 - listing, 500
 - requesting
 - from CA, 501
 - on hardware, 507
 - storing
 - IKE, 532
 - on computer, 496
 - on hardware, 481, 520
- Challenge label, 602, 624
- changing, privilege level in IKE, 493
- Changing IKE Transmission Parameters task map, 523
- ciphers, *See* encryption algorithms
- class A, B, and C network numbers, 54, 59
- class A network numbers
 - description, 202
 - IPv4 address space division, 59
 - range of numbers available, 59
- class B network numbers
 - description, 203
 - IPv4 address space division, 59
 - range of numbers available, 59
- class C network numbers
 - description, 203
 - IPv4 address space division, 59
 - range of numbers available, 59
- `class` clause, in the IPQoS configuration file, 721
- `class` clause, in the IPQoS configuration file, 772

- class of service (CoS) mark, 689
- classes, 687
 - defining, in the IPQoS configuration file, 729, 733
 - selectors, list of, 758
 - syntax of `class` clause, 772
- classes of service, *See* classes
- classifier module, 687
 - action statement, 720
 - functions of the classifier, 758
- colocated care-of address, 586, 593, 596
 - acquiring, 588
- color awareness, 689, 761
- commands
 - IKE, 530-532
 - `ikeadm` command, 482, 493, 528
 - `ikecert` command, 482, 528, 530
 - `in.iked` daemon, 527
 - IPsec
 - `in.iked` command, 431
 - `ipsecalgs` command, 434, 472
 - `ipseconf` command, 439, 447, 469-470
 - `ipseckey` command, 439, 462, 473-474
 - list of, 439-440
 - security considerations, 473
 - `snoop` command, 475
- computations
 - accelerating IKE in hardware, 481, 521-522, 522-523
- configuration files
 - creating for Solaris IP Filter, 572-573
 - IPv6
 - `/etc/inet/hostname6.interface` file, 215-216
 - `/etc/inet/ipaddrsel.conf` file, 216
 - `/etc/inet/ndpd.conf` file, 211-215, 214
 - Solaris IP Filter examples, 536-537
 - TCP/IP networks
 - `/etc/defaultdomain` file, 185
 - `/etc/defaultrouter` file, 185
 - `/etc/hostname.interface` file, 184
 - `/etc/nodename` file, 106, 184
 - hosts database, 185, 188
 - netmasks database, 188
- configuring
 - address pools, 541-542
 - DHCP client, 373
- configuring (Continued)
 - DHCP service, 279
 - IKE, 485
 - `ike/config` file, 528
 - IKE with CA certificates, 501-506
 - IKE with certificates on hardware, 506-510
 - IKE with mobile systems, 513-520
 - IKE with public key certificates, 496, 497-501
 - IKE with self-signed certificates, 497-501
 - interfaces manually, for IPv6, 128-129
 - IPsec, 469-470
 - `ipseccinit.conf` file, 470-471
 - IPv6-enabled routers, 126
 - NAT rules, 540-541
 - network configuration server, 104
 - network security with a role, 467-468
 - packet filtering rules, 537-540
 - routers, 201
 - network interfaces, 118, 120
 - overview, 118
 - TCP/IP configuration files, 183
 - `/etc/defaultdomain` file, 185
 - `/etc/defaultrouter` file, 185
 - `/etc/hostname.interface` file, 184
 - `/etc/nodename` file, 106, 184
 - hosts database, 185, 188
 - netmasks database, 188
 - TCP/IP configuration modes
 - local files mode, 97, 104
 - mixed configurations, 98
 - network client mode, 106
 - sample network, 99
 - TCP/IP networks
 - configuration files, 183
 - local files mode, 104
 - network clients, 105
 - network databases, 192, 195, 197
 - `nsswitch.conf` file, 195, 197
 - prerequisites, 96
 - standard TCP/IP services, 108
 - VPN protected by IPsec, 450-456, 456-460
 - Configuring IKE for Mobile Systems task map, 512
 - Configuring IKE task map, 485
 - Configuring IKE to Find Attached Hardware task map, 520
 - Configuring IKE With Public Key Certificates task map, 496

- connectivity, ICMP protocol reports of
 - failures, 39
- converting DHCP data store, 363-365
- CRC (cyclical redundancy check) field, 46
- creating
 - certificate requests, 501
 - DHCP macros, 346
 - DHCP options, 353
 - IPsec SAs, 446, 461-465
 - ipseccinit.conf file, 446
 - security parameter index (SPI), 461
 - security-related role, 467-468
 - self-signed certificates (IKE), 497
- CRLs
 - accessing from central location, 510
 - ignoring, 504
 - ike/crls database, 532
 - ikecert certrldb command, 532
 - listing, 510
- cyclical redundancy check (CRC) field, 46

D

- D option
 - ikecert certlocal command, 497
 - ikecert command, 531
- daemons
 - in.iked daemon, 478, 482, 527
 - in.mpathd daemon, 638
 - in.ndpd daemons, 222
 - in.ripngd daemon, 126, 223
 - in.routed routing daemon, 107
 - in.tftpd daemon, 104
 - inetd Internet services, 192
 - network configuration server booting
 - protocols, 98
- data addresses, IPMP, definition, 642
- data communications, 43, 47
 - packet life cycle, 44, 47
- data encapsulation
 - definition, 43
 - TCP/IP protocol stack and, 43, 47
- data-link layer
 - framing, 46
 - OSI, 37
 - packet life cycle
 - receiving host, 46

- data-link layer, packet life cycle (Continued)
 - sending host, 46
 - TCP/IP, 37, 38
- databases
 - IKE, 530-532
 - ike/crls database, 532
 - ike.privatekeys database, 530, 532
 - ike/publickeys database, 531, 532
 - security associations database (SADB), 472
 - security policy database (SPD), 426
- datagrams
 - IP, 425
 - IP header, 46
 - IP protocol formatting, 38
 - packet process, 46
 - UDP protocol functions, 40
- deactivating Solaris IP Filter, 552-554, 554
- decimal to binary conversion, 190
- default address selection, 216-217
 - definition, 173-176
 - IPv6 address selection policy table, 174-175
- default mobile node
 - Mobile IP Address section, 604, 629-630
- defaultdomain file
 - deleting for network client mode, 106
 - description, 185
 - local files mode configuration, 103
- defaultrouter file
 - automatic router protocol selection and, 107
 - description, 185
 - local files mode configuration, 103
- deleting
 - DHCP options, 358
 - IPsec SAs, 462
- deprecated attribute, ifconfig
 - command, 644
- deregistering
 - Mobile IP, 586, 591, 592
- DES encryption algorithm, IPsec and, 434
- designing the network
 - domain name selection, 63
 - IP addressing scheme, 54, 61
 - naming hosts, 62
 - overview, 53
 - subnetting, 188
- DHCP client
 - administration, 377
 - client ID, 326

DHCP client (Continued)

- definition, 261
 - disabling, 376
 - displaying interface status, 378
 - dropping IP address, 377
 - enabling, 375-376
 - event scripts, 386-388
 - extending lease, 377
 - host name
 - specifying, 380-381
 - host name generation, 272
 - incorrect configuration, 404
 - logical interfaces, 379
 - management of network interface, 374
 - multiple network interfaces, 379
 - name services, 308
 - network information without lease, 362-363, 377
 - on diskless client systems, 361
 - option information, 359
 - parameters, 378-379
 - releasing IP address, 377
 - running in debugging mode
 - sample output, 398
 - running programs with, 386-388
 - shutdown, 375
 - starting, 377
 - startup, 374
 - testing interface, 377
 - troubleshooting, 395
 - unconfiguring, 376
- ## DHCP command-line utilities, 255
- privileges, 295
- ## DHCP Configuration Wizard
- description, 280
 - for BOOTP relay agent, 284
- ## DHCP data store
- choosing, 269
 - converting, 363-365
 - exporting data, 367, 368-369
 - importing data, 369
 - modifying imported data, 370
 - moving data between servers, 365-371
 - overview, 253
- ## DHCP events, 386-388
- ## DHCP lease
- and reserved IP addresses, 274
 - dynamic and permanent, 273

DHCP lease (Continued)

- expiration date, 327
 - negotiation, 270
 - policy, 269
 - reserved IP addresses, 327
 - time, 270
 - type, 327
- ## DHCP macros
- automatic processing, 259
 - categories, 259
 - client class macros, 259
 - client ID macros, 259
 - configuration, 326
 - creating, 346
 - default, 272
 - deleting, 349
 - Locale macro, 281
 - modifying, 342
 - network address macro, 259, 282
 - network booting, 361
 - order processed, 260
 - overview, 259
 - server macro, 282
 - size limit, 260
 - working with, 340
- ## DHCP Manager
- description, 255
 - features, 276
 - menus, 293
 - starting, 294
 - stopping, 295
 - window and tabs, 292
- ## DHCP network tables
- created during server configuration, 282
 - description, 254
 - removing when unconfiguring, 285
- ## DHCP Network Wizard, 314
- ## DHCP networks
- adding to DHCP service, 314
 - modifying, 317
 - removing from DHCP service, 319
 - working with, 311-321
- ## DHCP options
- creating, 353
 - deleting, 358
 - modifying, 356
 - overview, 258
 - properties, 351

- DHCP options (Continued)
 - working with, 350
- DHCP protocol
 - advantages in Solaris implementation, 248
 - overview, 247
 - sequence of events, 249
- DHCP server
 - configuration
 - information gathered, 266
 - overview, 257
 - configuring
 - dhcpconfig command, 287-288
 - with DHCP Manager, 280
 - data store, 253
 - enabling to update DNS, 305-306
 - functions, 252
 - how many to configure, 265
 - management, 253
 - options, 299
 - DHCP Manager, 310
 - dhcpconfig command, 310-311
 - planning for multiple servers, 274
 - running in debugging mode, 397
 - sample output, 398-401
 - selecting, 268
 - troubleshooting, 389
- DHCP service
 - adding networks to, 314
 - cache offer time, 309
 - enabling and disabling
 - DHCP Manager, 297
 - dhcpconfig command, 297-298
 - effects of, 296
 - error messages, 392, 400
 - IP address allocation, 257
 - IP addresses
 - adding, 328
 - modifying properties, 332
 - removing, 334
 - reserving for client, 337
 - unusable, 334
 - logging
 - overview, 301
 - transactions, 302
 - modifying service options, 299
 - network configuration overview, 258
 - network interface monitoring, 312-313
 - network topology, 264
- DHCP service (Continued)
 - planning, 263
 - Service Management Facility, 298-299
 - Solaris network boot and install, 360
 - starting and stopping
 - DHCP Manager, 297
 - effects of, 296
 - supporting BOOTP clients, 321
 - unconfiguring, 285
 - with DHCP Manager, 286
 - WAN boot installation support, 360
- dhcpagent daemon, 374
 - debugging mode, 396
 - parameter file, 418
- dhcpconfig command
 - description, 256, 410
- dhcpinfo command, description, 410
- dhcpcmgr command, description, 410
- dhcpsvc.conf file, 417
- dhcptab table, 281
 - description, 417
 - overview, 253
 - reading automatically, 309
 - removing when unconfiguring, 285
- dhcptags file, 418
- dhtadm command
 - creating macros with, 346
 - creating options with, 353
 - deleting macros with, 349
 - deleting options with, 358
 - description, 256, 409
 - modifying macros with, 342
 - modifying options with, 356
- differentiated services, 681
 - differentiated services model, 687
 - network topologies, 696
 - providing different classes of service, 686
- Diffserv-aware router
 - evaluating DS codepoints, 764
 - planning, 701
- Diffserv model
 - classifier module, 687
 - flow example, 690
 - IPQoS implementation, 687, 688, 689, 690
 - marker modules, 689
 - meter modules, 688
- digital signatures
 - DSA, 531

- digital signatures (Continued)
 - RSA, 531
 - directories
 - certificates (IKE), 532
 - /etc/inet, 482
 - /etc/inet/ike, 482
 - /etc/inet/publickeys, 532
 - /etc/inet/secret, 482
 - /etc/inet/secret/ike.privatekeys, 530
 - presared keys (IKE), 529
 - private keys (IKE), 530
 - public keys (IKE), 532
 - directory name (DN), for accessing CRLs, 510
 - diskless clients, DHCP support of, 361
 - displaying
 - configuration information, 153
 - IPsec policy, 449
 - status, 153
 - dlcosmk marker, 689
 - planning datagram forwarding, 709
 - user priority values, table of, 765
 - VLAN tags, 765
 - domain name system (DNS)
 - description, 41
 - domain name registration, 36
 - enabling dynamic updates by DHCP server, 305-306
 - extensions for IPv6, 242
 - network databases, 63, 193
 - preparing, for IPv6 support, 91
 - reverse zone file, 138
 - selecting as name service, 63
 - zone file, 138
 - domain names
 - /etc/defaultdomain file, 103, 106, 185
 - registering, 36
 - selecting, 63
 - top-level domains, 64
 - dotted-decimal format, 57
 - dropped or lost packets, 39, 164
 - DS codepoint (DSCP), 689, 691
 - AF forwarding codepoint, 692, 764
 - color-awareness configuration, 762
 - configuring, on a diffserv router, 741, 763
 - defining, in the IPQoS configuration file, 725
 - dscp_map parameter, 765
 - EF forwarding codepoint, 692, 764
 - PHBs and the DSCP, 692
 - DS codepoint (DSCP) (Continued)
 - planning, in the QoS policy, 709
 - dscpmk marker, 689
 - invoking, in a marker action statement, 724, 730, 736, 739
 - PHBs for packet forwarding, 763
 - planning packet forwarding, 708
 - DSS authentication algorithm, 531
 - dual-stack protocols, 88, 210-211
 - duplicate address detection
 - algorithm, 229
 - DHCP service, 309
 - IPv6, 81
 - Dynamic Host Configuration Protocol, *See* DHCP protocol
 - dynamic interfaces
 - agent advertisement over, 587, 621
 - dynamic reconfiguration (DR)
 - adding interfaces to an IPMP group, 650
 - definition, 641
 - detaching interfaces to an IPMP group, 651
 - DR-attach procedures, 673-674
 - DR-detach procedures, 672-673
 - interfaces not present at boot time, 651-652
 - interoperation with IPMP, 649-652
 - reattaching interfaces in an IPMP group, 651
 - replacing an interface not present at boot time, 674-676
 - replacing failed interfaces, 672-674
 - dynamic routing, 107
- E**
- enabling Solaris IP Filter, 546-548
 - encapsulated datagram, Mobile IP, 584
 - encapsulating security payload (ESP)
 - description, 432-433
 - IPsec protection mechanism, 432-434
 - protecting IP packets, 425
 - security considerations, 433
 - encapsulation types, Mobile IP, 595
 - encr_algs security option, ifconfig command, 475
 - encr_auth_algs security option, ifconfig command, 475

- encryption algorithms
 - IPsec
 - 3DES, 434
 - AES, 434
 - Blowfish, 434
 - DES, 434
 - specifying for IPsec, 474
 - error messages for IPQoS, 747
 - ESP, *See* encapsulating security payload (ESP)
 - /etc/bootparams file, 197
 - /etc/default/dhcpagent file, 378-379
 - /etc/default/dhcpagent file,
 - description, 418
 - /etc/default/inet_type file, 165-166
 - DEFAULT_IP value, 221
 - /etc/default/mpathd file, 677
 - /etc/defaultdomain file
 - deleting for network client mode, 106
 - description, 185
 - local files mode configuration, 103
 - /etc/defaultrouter file
 - description, 185
 - local files mode configuration, 103
 - /etc/dhcp/dhcptags file
 - converting entries, 418
 - description, 418
 - /etc/dhcp/eventhook file, 386
 - /etc/dhcp/inittab file
 - description, 418
 - modifying, 359
 - /etc/dhcp/interface.dhc file, description, 418
 - /etc/dhcp.interface file, 374, 378
 - /etc/dhcp.interface file, description, 417
 - /etc/ethers file, 198
 - /etc/hostname.interface file
 - description, 184
 - local files mode configuration, 102
 - /etc/hostname.interface file, manual configuration, 114
 - /etc/hostname.interface file, network client mode configuration, 106
 - /etc/hostname.interface file
 - router configuration, 119
 - /etc/hostname6.interface file, IPv6 tunneling, 235
 - /etc/hostname6.interface file, manually configuring interfaces, 128-129
 - /etc/hostname6.interface file,
 - syntax, 215-216
 - /etc/hostname6.ip.6to4tun0 file, 134
 - /etc/hostname6.ip.tun file, 131, 132, 133
 - /etc/hosts file, *See* /etc/inet/hosts file
 - /etc/inet/dhcpsvc.conf file, 281
 - /etc/inet/hosts file, 445
 - adding subnets, 99
 - format, 185
 - host name, 186
 - initial file, 186, 187
 - local files mode configuration, 103
 - loopback address, 186
 - multiple network interfaces, 187
 - network client mode configuration, 106
 - /etc/inet/ike/config file
 - cert_root keyword, 503, 508
 - cert_trust keyword, 499, 508
 - description, 480, 528
 - ignore_crls keyword, 504
 - ikecert command and, 530
 - ldap-list keyword, 511
 - PKCS #11 library entry, 530
 - pkcs11_path keyword, 506, 521, 522, 530
 - preshared keys, 487
 - proxy keyword, 511
 - public key certificates, 503, 508
 - putting certificates on hardware, 508
 - sample, 487
 - security considerations, 528
 - self-signed certificates, 499
 - summary, 482
 - transmission parameters, 524
 - use_http keyword, 511
 - /etc/inet/ike/crls directory, 532
 - /etc/inet/ike/publickeys directory, 532
 - /etc/inet/ipaddrsel.conf file, 174, 216
 - /etc/inet/ipnodes file, 241, 242, 445
 - /etc/inet/ipsecinit.conf file, 470-471
 - /etc/inet/ipsecpolicy.conf file, 469-470
 - /etc/inet/ndpd.conf file, 127, 223
 - 6to4 advertisement, 206
 - 6to4 router advertisement, 135
 - creating, 127
 - interface configuration variables, 212
 - keywords, 211-215, 223
 - prefix configuration variables, 214
 - temporary address configuration, 145

- /etc/inet/netmasks file
 - adding subnets, 99
 - editing, 191
 - router configuration, 120
- /etc/inet/networks file, overview, 199
- /etc/inet/protocols file, 200
- /etc/inet/secret/ike.privatekeys directory, 532
- /etc/inet/services file, sample, 200
- /etc/ipf/ipf.conf file, *See* Solaris IP Filter
- /etc/ipf/ipnat.conf file, *See* Solaris IP Filter
- /etc/ipf/ippool.conf file, *See* Solaris IP Filter
- /etc/netmasks file, 191
- /etc/nodename file
 - deleting for network client mode, 106
 - description, 184
- /etc/nsswitch.conf file, 195, 197
 - changing, 196, 197
 - examples, 196
 - modifications, for IPv6 support, 242-243
 - name service templates, 196
 - network client mode configuration, 106
 - syntax, 196
 - use by DHCP, 417
- /etc/resolv.conf file, use by DHCP, 417
- Ethernet addresses
 - See* ethers database
 - See* MAC address
- ethers database
 - checking entries, 178
 - corresponding name service files, 194
 - overview, 198
- eventhook file, 386
- example IPQoS configuration files
 - application server, 731
 - best-effort web server, 719
 - color-awareness segment, 761
 - premium web server, 718
 - VLAN device configuration, 766
- expedited forwarding (EF), 692, 764
 - defining, in the IPQoS configuration file, 726
- expire_timer keyword, IKE configuration file, 524
- extending DHCP lease, 377

F

- f option
 - in.iked daemon, 488
 - ipseckey command, 447
- failback
 - definition, 640
 - dynamic reconfiguration (DR), with, 651
- failover
 - definition, 640
 - dynamic reconfiguration (DR), and, 651
 - examples, 648
 - standby interface, 645
- failover option, ifconfig command, 643
- failure detection, in IPMP, 646
 - definition, 640
 - NICs missing at boot time, 651-652
 - probing rate, 638
- failure detection time, IPMP, 647
- file services, 42
- files
 - IKE
 - crls directory, 482, 532
 - ike/config file, 440, 480, 482, 528
 - ike.preshared file, 482, 529
 - ike.privatekeys directory, 482, 532
 - publickeys directory, 482, 532
 - IPsec
 - /etc/inet/ipsecpolicy.conf file, 469-470
 - ipseccinit.conf file, 439, 470-471
 - ipseckey file, 439
 - ipsecpolicy.conf file, 439
- filter clause, in the IPQoS configuration file, 723, 773
- filters, 688
 - creating, in the IPQoS configuration file, 729, 734
 - filter clause syntax, 773
 - planning, in the QoS policy, 704
 - selectors, list of, 758
- flow accounting, 752, 767
 - flow record table, 768
- flow control, through the metering modules, 688
- flowacct module, 689, 767
 - acctadm command, for creating a flow accounting file, 769
 - action statement for flowacct, 727

- flowacct module (Continued)
 - attributes of flow records, 768
 - flow record table, 768
 - flow records, 752
 - parameters, 767
- flushing, *See* deleting
- foreign agent
 - authentication, 607
 - care-of address, 588, 591, 596
 - considerations, 594
 - datagrams, 583
 - definition, 583
 - determining functionality, 601
 - encapsulation support, 595
 - functioning without, 588
 - implementation, 615
 - message authentication, 626, 627
 - registering by using, 591
 - registering with multiple, 591
 - registration message, 586
 - relaying registration request, 593
 - requesting service from, 594
 - security association support, 593
 - serving mobile nodes, 587
 - visitor list, 612, 631
- foreign network, 584, 591, 596
- ForeignAgent label, 602, 611, 621, 622
- forwarding traffic
 - datagram forwarding, 765
 - effect of PHBs on packet forwarding, 763
 - IP packet forwarding, with DSCP, 691
 - planning, in the QoS policy, 703
 - traffic flow through Diffserv networks, 693
- fragmented packets, 38
- framing
 - data-link layer, 38, 46
 - description, 46
- ftp program, 40
 - anonymous FTP program
 - description, 41

G

- General section
 - Mobile IP configuration file, 621
 - Version label, 621
- generating, random numbers, 460-461

- gethostbyname command, 243
- getipnodebyname command, 243
- GlobalSecurityParameters section
 - labels and values, 624
 - Mobile IP configuration file, 623-624
- group failures, IPMP, 647
- group parameter
 - ifconfig command, 659, 671

H

- HA-FAauth label, 602, 607, 624
- handshake, three-way, 45
- hardware
 - accelerating IKE computations, 481, 521-522
 - physical layer (OSI), 37
 - physical network layer (TCP/IP), 37, 38
 - storing IKE keys, 481, 522-523
- hardware for IPQoS-enabled networks, 696
- header fields, IPv6, 209
- header of packets
 - IP header, 46
 - TCP protocol functions, 39
- home address, 582, 584
- home agent
 - Address section, 626, 627
 - authentication, 607
 - binding table, 612, 614, 631
 - considerations, 594
 - delivery of datagram, 583
 - deregistering, 591
 - determining functionality, 601
 - dynamic address assignment, 624
 - dynamic discovery, 595
 - encapsulation, 595
 - forwarding datagrams, 596
 - implementation, 615
 - message replay protection, 623
 - mobile node location, 586
 - registration message, 586, 591
 - registration reply, 594
 - registration request, 593, 594
 - security association support, 593
 - state information, 632
- home-foreign agent authentication, 593
- home network, 583, 584, 591, 594
- HomeAgent label, 602, 611, 621, 622

- hops, relay agent, 309
- host, configuring a 6to4 address, 207
- host configuration modes (TCP/IP), 97, 99
 - IPv4 network topology, 99
 - local files mode, 97, 98
 - mixed configurations, 98
 - network client mode, 98
 - network configuration servers, 98
 - sample network, 99
- host name, enabling client request of, 380-381
- host-to-host communications, 38
- hostconfig program, 106
- hostname.*interface* file
 - description, 184
- hostname.*interface* file, in IPMP, 666
- hostname.*interface* file
 - router configuration, 119
- hostname6.*interface* file, manually
 - configuring interfaces, 128-129
- hostname6.*interface* file, syntax, 215-216
- hostname6.*ip.tun* file, 131, 132, 133
- hosts
 - checking host connectivity with ping, 164
 - checking IP connectivity, 165
 - configuring for IPv6, 142-147
 - host name
 - administering, 62
 - /etc/inet/hosts file, 186
 - in an IPv4 network topology, 99
 - multihomed
 - creating, 121
 - receiving
 - packet travel through, 46, 47
 - routing protocol selection, 120
 - sample network, 99
 - sending
 - packet travel through, 44, 46
 - TCP/IP configuration modes, 99
 - configuration information, 97
 - local files mode, 97, 98, 104
 - mixed configurations, 98
 - network client mode, 98, 106
 - network configuration servers, 98
 - sample network, 99
 - temporary IPv6 addresses, 144-147
 - troubleshooting general problems, 177
- hosts.byaddr map, 139, 242
- hosts.byname map, 139, 242
- hosts database, 185, 188
 - checking entries, 178
 - corresponding name service files, 194
 - /etc/inet/hosts file
 - adding subnets, 99
 - format, 185
 - host name, 186
 - initial file, 186, 187
 - local files mode configuration, 103
 - loopback address, 186
 - multiple network interfaces, 187
 - network client mode configuration, 106
 - router configuration, 120
 - name service
 - affect on, 187
 - forms of, 193
 - name services' affect, 188
- hosts file, 445
- hosts.org_dir table, 139
- http access to CRLs, use_http keyword, 511

I

- ICMP protocol
 - description, 39
 - displaying statistics, 157
 - invoking, with ping, 164
 - messages, for Neighbor Discovery
 - protocol, 226
- ICMP Router Discovery (RDISC) protocol, 201
- ifconfig command, 235, 536
 - 6to4 extensions, 134
 - a option, 143
 - auth_algs security option, 474-475
 - checking order of STREAMS modules, 656
 - configuring
 - IPv6 tunnels, 220
 - VLAN devices, 117
 - controlling DHCP client, 377
 - deprecated attribute, 644
 - description, 153
 - DHCP and, 410
 - displaying interface status, 153, 155-156, 645
 - displaying IPMP group, 669
 - encr_algs security option, 475
 - encr_auth_algs security option, 475
 - failover option, 643

- ifconfig command (Continued)
 - group parameter, 659, 671
 - information in output, 154
 - IPMP extensions to, 638
 - IPsec security options, 474-475
 - IPv6 extensions to, 219
 - output format, 153
 - setting tunnels, 435
 - standby parameter, 645, 666
 - syntax, 153
 - test parameter, 659
 - use as troubleshooting tool, 177
- ignore_crls keyword, IKE configuration file, 504
- IKE
 - adding self-signed certificates, 497
 - certificates, 480
 - checking if valid policy, 488
 - command descriptions, 482
 - configuration files, 482
 - configuring
 - for mobile systems, 513-520
 - with CA certificates, 501-506
 - with preshared keys, 486
 - with public key certificates, 496
 - creating self-signed certificates, 497
 - crls database, 532
 - daemon, 527
 - databases, 530-532
 - /etc/inet/ike/config file, 521, 522
 - finding attached hardware, 520
 - generating certificate requests, 501
 - hardware acceleration, 481
 - hardware storage of keys, 481
 - ike.preshared file, 529
 - ike.privatekeys database, 532
 - ikeadm command, 528
 - ikecert certadb command, 502
 - ikecert certrldb command, 512
 - ikecert command, 530
 - ikecert tokens command, 523
 - implementing, 485
 - in.iked daemon, 527
 - ISAKMP SAs, 479
 - key management, 478
 - mobile systems and, 513-520
 - NAT and, 516-517, 518-519
 - overview, 477

- IKE (Continued)
 - perfect forward secrecy (PFS), 478
 - Phase 1 exchange, 479
 - Phase 1 key negotiation, 524-526
 - Phase 2 exchange, 479
 - PKCS #11 library, 522, 531
 - preshared keys, 480
 - privilege level
 - changing, 493
 - checking, 490, 495
 - lowering, 493
 - publickeys database, 532
 - reference, 527
 - RFCs, 427
 - security associations, 527
 - storage locations for keys, 482
 - troubleshooting transmission timing, 524-526
 - using Sun Crypto Accelerator 1000 board, 521-522
 - using Sun Crypto Accelerator 4000 board, 522-523
 - ike/config file, *See* /etc/inet/ike/config file
 - ike_mode keyword, ikeadm command, 493
 - ike.preshared file, 489, 529
 - sample, 494
 - ike.privatekeys database, 532
 - ikeadm command
 - description, 528
 - interactive mode, 493
 - privilege level
 - changing, 493
 - checking, 490, 495
 - ikecert certadb command
 - a option, 499, 502
 - ikecert certlocal command
 - kc option, 501
 - ks option, 497
 - ikecert certrldb command, -a option, 512
 - ikecert command
 - A option, 531
 - a option, 506
 - description, 528, 530
 - T option, 506, 531
 - t option, 531
 - ikecert tokens command, 523
 - in.dhcpd daemon, 256

- in.dhcpd daemon (Continued)
 - debugging mode, 397
 - description, 410
- in.iked daemon
 - activating, 527
 - c option, 488
 - description, 478
 - f option, 488
 - privilege level
 - changing, 493
 - checking, 490, 495
 - stop and start, 447, 490
- in.mpathd daemon
 - definition, 638
 - probing rate, 638
 - probing targets, 647
- in.ndpd daemon
 - checking the status, 178
 - creating a log, 167-168
 - options, 222
- in.rarpd daemon, 98
- in.rdisc program, description, 202
- in.ripngd daemon, 126, 223
- in.routed daemon, 107
 - creating a log, 166-167
 - description, 201
 - space-saving mode, 201
- in.telnet daemon, 41
- in.tftpd daemon
 - description, 98
 - turning on, 104
- inactive rule sets, *See* Solaris IP Filter
- inbound load balancing, 230
- inet_type file, 165-166
- inetd daemon
 - administering services, 192
- inetd daemon, checking the status, 178
- inetd daemon
 - IPv6 services and, 224-225
 - services started by, 108
- interactive mode
 - ikeadm command, 493
 - ipseckey command, 462
- interface ID
 - definition, 78
 - format, in an IPv6 address, 75
 - using a manually-configured token, 147
- interfaces
 - checking packets, 170-171
 - configuring
 - after installation, 113
 - IPv6 logical interfaces, 215-216
 - manually, for IPv6, 128-129
 - temporary addresses, 144-147
 - displaying status, 645
 - failover, with IPMP, 648
 - IPMP interface types, 644-645
 - multihomed hosts, 121, 187
 - order of STREAMS modules on an
 - interface, 656
 - pseudo-interface, for 6to4 tunnels, 134
 - removing, 115
 - router configuration, 118, 120
 - standby, in IPMP, 644-645, 665-667
 - types of NICs, 113
 - VLANs, 115-118
- Internet, domain name registration, 36
- Internet Assigned Numbers Authority (IANA),
 - registration services, 59
- Internet drafts
 - definition, 48
 - SCTP with IPsec, 427
- Internet layer (TCP/IP)
 - ARP protocol, 39
 - description, 37, 38
 - ICMP protocol, 39
 - IP protocol, 38
 - packet life cycle
 - receiving host, 46
 - sending host, 45
- Internet Protocol (IP), 581
- Internet Security Association and Key Management Protocol (ISAKMP) SAs
 - description, 479
 - storage location, 529
- internetworks
 - definition, 65
 - packet transfer by routers, 66, 67
 - redundancy and reliability, 65
 - topology, 65
- InterNIC
 - registration services
 - domain name registration, 36
- IP address
 - BaseAddress label, 624

- IP address (Continued)
 - care-of address, 588
 - IP source address, 596
 - mobile node, 584, 593
 - source IP address, 597
- IP addresses
 - allocation with DHCP, 271
 - designing an address scheme, 54, 61
 - DHCP
 - adding, 328
 - errors, 392
 - modifying properties, 332
 - properties, 325
 - removing, 334
 - reserving for client, 337
 - tasks, 324
 - unusable, 334
 - displaying addresses of all interfaces, 155-156
 - IP protocol functions, 38
 - network classes
 - network number administration, 54
 - network interfaces and, 61
 - subnet issues, 190
- IP datagrams
 - IP header, 46
 - IP protocol formatting, 38
 - packet process, 46
 - protecting with IPsec, 425
 - UDP protocol functions, 40
- IP forwarding
 - in IPv4 VPNs, 452, 454
 - in IPv6 VPNs, 457, 459
 - in VPNs, 436
- IP link, in IPMP terminology, 639
- IP network multipathing (IPMP), *See* IPMP
- IP protocol
 - checking host connectivity, 164, 165
 - description, 38
 - displaying statistics, 157
- IP security architecture, *See* IPsec
- ipaddrsel command, 174, 216-217
- ipaddrsel.conf file, 174, 216
- ipf command
 - See also* Solaris IP Filter
 - a option, 556-557
 - append rules from command line, 558
 - D option, 554
- ipf command (Continued)
 - E option, 548-549
 - F option, 551, 556-557, 557-558, 560-561
 - f option, 548-549, 556-557, 558, 559
 - I option, 559, 560-561
 - s option, 559-560
- ipf.conf file, 537-540
 - See* Solaris IP Filter
- ipfstat command, 566-567
 - See also* Solaris IP Filter
 - I option, 556
 - i option, 556
 - o option, 556
 - s option, 567
 - t option, 566-567
- ipgpc classifier, *See* classifier module
- ipmon command
 - See also* Solaris IP Filter
 - a option, 569-570
 - F option, 570-571
 - o option, 569-570
- IPMP
 - administering, 668-671
 - ATM support, 657
 - basic requirements, 641
 - configuration
 - verifying MAC address uniqueness, 657-659
 - data addresses, 642
 - dynamic reconfiguration, 641, 649-652
 - Ethernet support, 657
 - failover
 - definition, 640
 - failure detection
 - definition, 640
 - failure detection time, 647
 - group configuration
 - planning for an IPMP group, 655-657
 - tasks for configuring, 659-663
 - troubleshooting, 662
 - hostname.*interface* file, 666
 - interface configuration
 - active-active, 645
 - active-standby, 645
 - standby interface, 644-645, 665-667
 - types of interface configurations, 644
 - IP links, types of, 639
 - IPMP configuration file, 677

- IPMP (Continued)
 - link-based failure detection, 646
 - load spreading, 638
 - multipathing group definition
 - See IPMP group
 - network drivers supported, 646
 - overview, 637-641
 - preserving configuration across reboots, 661, 662, 666
 - probe-based failure detection, 647
 - probe traffic, 642
 - repair detection, 640
 - replacing an interface not present at system boot, 674-676
 - replacing interfaces, DR, 672-674
 - software components, 638
 - target systems, 640
 - configuring in a script, 664-665
 - configuring manually, 663-664
 - terminology, 638-641
 - test addresses, 642-643
 - Token ring support, 657
- IPMP daemon in `mpathd`, 638
- IPMP groups
 - adding an interface to a group, 669-670
 - adding interfaces, through DR, 650
 - affect of interfaces not present at boot time, 651-652
 - configuring, 659-663
 - configuring a group for a single interface, 667-668
 - displaying group membership, 669
 - group failures, 647
 - moving an interface between groups, 671
 - NIC speed in a group, 639-640
 - planning tasks, 655-657
 - removing an interface from a group, 670-671
 - removing interfaces, through DR, 651
 - troubleshooting group configuration, 662
- `ipnat` command
 - See also Solaris IP Filter
 - append rules from command line, 562-563
 - C option, 552
 - F option, 552, 562
 - f option, 548-549, 562-563
 - l option, 561-562
 - s option, 567-568
- `ipnat.conf` file, 540-541
- `ipnat.conf` file (Continued)
 - See Solaris IP Filter
- `ipnodes.byaddr` map, 139
- `ipnodes.byname` map, 139
- `ipnodes` file, 241, 445
- `ipnodes.org_dir` table, 139
- `ippool` command
 - See also Solaris IP Filter
 - append rules from command line, 564-565
 - F option, 564
 - f option, 564-565
 - l option, 563-564
 - s option, 568
- `ippool.conf` file, 541-542
 - See Solaris IP Filter
- IPQoS, 681
 - configuration example, 711-713
 - configuration file, 717, 770
 - action statement syntax, 772
 - class clause, 721
 - filter clause, 723
 - initial action statement, 771
 - initial action statement, 720
 - list of IPQoS modules, 772
 - marker action statement, 724
 - syntax, 770
 - configuration planning, 695
 - Diffserv model implementation, 687
 - error messages, 747
 - features, 682
 - man pages, 683
 - message logging, 746
 - network example, 717
 - network topologies supported, 696, 697, 698
 - policies for IPv6-enabled networks, 91
 - QoS policy planning, 699
 - related RFCs, 683
 - routers on an IPQoS network, 741
 - statistics generation, 754
 - traffic management capabilities, 685, 686
 - VLAN device support, 765
- `ipqosconf`, 717
- `ipqosconf` command
 - applying a configuration, 744, 745
 - command options, 774
 - listing the current configuration, 745
- IPsec
 - activating, 439

IPsec (Continued)

- adding security associations (SAs), 446
- algorithm source, 472
- authentication algorithms, 434
- bypassing, 435, 448
- commands, list of, 439-440
- components, 425
- configuration files, 439-440
- configuring, 434, 469-470
- creating SAs manually, 461-465
- displaying policies, 449
- encapsulating data, 432
- encapsulating security payload (ESP), 432-434
- encryption algorithms, 434
- /etc/hosts file, 445
- /etc/inet/ipnodes file, 445
- /etc/inet/ipsecpolicy.conf file, 469-470
- extensions to utilities
 - ifconfig command, 474-475
 - snoop command, 475
- getting random numbers for keys, 460-461
- ifconfig command
 - configuring VPN, 454, 458
 - security options, 474-475
 - setting policy, 469-470
- implementing, 443
- in.iked daemon, 431
- inbound packet process, 428
- ipsecalgs command, 434, 472
- ipseccomf command, 435, 469-470
- ipseccinit.conf file, 435
 - bypassing LAN, 456, 474
 - configuring, 446
 - description, 470-471
 - protecting web server, 448
- ipseckey command, 431, 473-474
- key management, 431-432
- keying utilities
 - IKE, 478
 - ipseckey command, 473-474
- Mobile IP, 598
- NAT and, 437-438
- outbound packet process, 428
- overview, 425
- policy command, 469-470
- policy files, 470-471

IPsec (Continued)

- protecting
 - mobile systems, 513-520
 - packets, 425
 - VPNs, 450-456
 - web servers, 447-449
- protection mechanisms, 432-434
- protection policy, 434-435
- RBAC and, 444
- replacing security associations (SAs), 462
- RFCs, 427
- route command, 455, 459
- SCTP protocol and, 438, 444
- securing traffic, 445
- security associations (SAs), 431-432
- security associations database (SADB), 426, 472
- security mechanisms, 426
- security parameter index (SPI), 431-432
- security policy database (SPD), 426, 427, 469
- security protocols, 426, 431-432
- security roles, 467-468
- setting policy
 - permanently, 470-471
 - temporarily, 469-470
- snoop command, 475
- Solaris cryptographic framework and, 472
- specifying
 - authentication algorithms, 474
 - encryption algorithms, 474
- temporary policy file, 439
- terminology, 427-428
- transport mode, 435-436
- tunnel mode, 435-436
- tunnels, 436
- used with IPv4 VPN, 450-456
- used with IPv6 VPN, 456-460
- verifying packet protection, 465-467
- virtual private networks (VPN), 437, 450-456
- zones and, 439, 444

ipseccomf command

- a option, 447, 493
- configuring IPsec policy, 469-470
- description, 439
- displaying IPsec policy, 447-449, 449
- f option, 447
- purpose, 435
- security considerations, 447, 471

- ipseccinit.conf file
 - bypassing LAN, 456
 - configuring tunnel options, 474
 - description, 439
 - protecting web server, 448
 - purpose, 435
 - sample, 470
 - security considerations, 471
- ipseckey command
 - description, 439, 473-474
 - interactive mode, 462
 - purpose, 431
 - security considerations, 473
- ipseckey file, storing IPsec keys, 439
- ipsecpolicy.conf file, 469-470
- IPv4 addresses
 - applying netmasks, 190
 - dotted-decimal format, 57
 - format, 57
 - IANA network number assignment, 59
 - network classes, 59
 - addressing scheme, 58, 59
 - class A, 202
 - class B, 203
 - class C, 203
 - parts, 59
 - range of numbers available, 59
 - subnet issues, 189
 - subnet number, 59
 - symbolic names for network numbers, 191
- IPv6
 - 6to4 address, 206
 - adding
 - addresses to NIS, 139
 - DNS support, 138
 - address autoconfiguration, 222, 227
 - addressing plan, 94
 - ATM support, 244
 - automatic tunnels, 234
 - checking the status of `in.ndpd`, 178
 - comparison with IPv4, 70, 230-232
 - configuring tunnels, 130-131
 - default address selection policy table, 217
 - DNS AAAA records, 140
 - DNS support preparation, 91
 - dual-stack protocols, 88
 - duplicate address detection, 81
 - enabling, on a server, 147-149

- IPv6 (Continued)
 - `/etc/inet/ipnodes` file, 242
 - extension header fields, 210
 - extensions to `ifconfig` command, 219
 - `in.ndpd` daemon, 222
 - `in.ripngd` daemon, 223
 - known issues with 6to4 router, 180
 - link-local addresses, 228, 231
 - monitoring traffic, 173
 - multicast addresses, 207-208, 231
 - Neighbor Discovery protocol, 226-232
 - neighbor solicitation, 226
 - neighbor solicitation and unreachability, 229
 - neighbor unreachability detection, 81, 231
 - next-hop determination, 81
 - `nslookup` command, 140
 - packet header format, 208-210
 - protocol overview, 227
 - redirect, 81, 226, 231
 - router advertisement, 226, 227, 230, 233
 - router discovery, 222, 230
 - router solicitation, 226, 228
 - routing, 232
 - security considerations, 92
 - site-local addresses, 83
 - stateless address autoconfiguration, 228
 - subnets, 74
 - temporary address configuration, 144-147
 - troubleshooting common IPv6
 - problems, 179-181
 - tunnels, 235-237
- IPv6 addresses
 - address autoconfiguration, 81, 82-83
 - address resolution, 81
 - anycast, 80
 - interface ID, 78
 - link-local, 79
 - multicast, 80
 - unicast, 77-78
 - uniqueness, 228
 - use in VPN example, 456-460
- IPv6 features, Neighbor Discovery
 - functionality, 81
- IPv6 link-local address, with IPMP, 643

K

- kc option
 - ikecert certlocal command, 497, 501, 530
- Key label, 603, 608, 626
- key management
 - automatic, 478
 - IKE, 478
 - IPsec, 431-432
 - manual, 473-474
 - zones and, 444
- key negotiation, IKE, 524-526
- key storage
 - IPsec SAs, 439
 - ISAKMP SAs, 529
- KeyDistribution label, 602, 624
- keying utilities
 - IKE protocol, 477
 - ipseckey command, 431
- keys
 - automatic management, 478
 - creating for IPsec SAs, 461-465
 - generating random numbers for, 460-461
 - ike.privatekeys database, 532
 - ike/publickeys database, 532
 - managing IPsec, 431-432
 - manual management, 473-474
 - preshared (IKE), 480
 - storing (IKE)
 - certificates, 532
 - private, 530
 - public keys, 532
 - storing on hardware, 481
- keystore name, *See* token ID
- ks option
 - ikecert certlocal command, 497, 530
- kstat command, use with IPQoS, 754

L

- l option
 - ikecert certdb command, 500
 - ipseccconf command, 449
- ldap-list keyword, IKE configuration file, 511
- libraries
 - PKCS #11, 522, 531

- link, IPv6, 74
- link-based failure detection, definition, 646
- link-layer address change, 230
- link-local address
 - as an IPMP test address, 643
 - format, 79
 - manually configuring, with a token, 147
- link-local addresses
 - IPv6, 228, 231, 235
- listing
 - algorithms (IPsec), 433, 475
 - certificates (IPsec), 500, 510
 - CRL (IPsec), 510
 - hardware (IPsec), 523
 - token IDS (IPsec), 523
- load balancing
 - in an IPQoS-enabled network, 698
 - on an IPv6-enabled network, 230
- load spreading
 - definition, 638
 - outbound, 641
- local files mode
 - definition, 97
 - host configuration, 104
 - network configuration servers, 98
 - systems requiring, 97, 98
- local files name service
 - description, 63
 - /etc/inet/hosts file, 445
 - example, 188
 - format, 185
 - initial file, 186, 187
 - requirements, 187
 - /etc/inet/ipnodes file, 445
- local files mode, 97, 98
- network databases, 193
- log file, flushing in Solaris IP Filter, 570-571
- log files, viewing for Solaris IP Filter, 569-570
- logged packets, saving to a file, 571
- logical interfaces
 - definition, 112
 - DHCP client systems, 379
 - for IPv6 address, 215-216
 - for IPv6 tunnels, 131, 132, 133
- loopback address, 106, 186
- lost or dropped packets, 39, 164

M

- m option, `ikecert certlocal` command, 497
- MAC address
 - IPMP requirements, 641
 - IPv6 interface ID, 78
 - mapping to IP in `ethers` database, 198
 - used in DHCP client ID, 259
 - verifying uniqueness, 657-659
- machines, protecting communication, 445
- macros
 - DHCP
 - See* DHCP macros
- marker modules, 689
 - See also* `dlcosmk` marker
 - See also* `dscpmk` marker
 - PHBs, for IP packet forwarding, 692
 - specifying a DS codepoint, 765
 - support for VLAN devices, 765
- MaxClockSkew label, 602, 624
- maximum transmission unit (MTU), 231
- MD5 authentication algorithm, key length, 463
- media access control (MAC) address, *See* MAC address
- message authentication
 - Mobile IP, 593, 625, 627
- message replay protection, 623
- messages, router advertisement, 233
- metering modules
 - See also* `tokenmt` meter
 - See also* `tswtclmt` meter
 - introduction, 688
 - invoking, in the IPQoS configuration file, 738
 - outcomes of metering, 688, 760
- `mipagent.conf` configuration file, 601, 602, 616, 630, 632
 - configuring, 600
- `mipagent` daemon, 601, 616, 632
- `mipagent_state` file, 632
- `mipagentconfig` command
 - configuring mobility agent, 630
 - description of commands, 630
 - modifying
 - Address section, 609
 - Advertisements section, 607
 - configuration file, 606
 - General section, 606
- `mipagentconfig` command, modifying (Continued)
 - GlobalSecurityParameters section, 607
 - Pool section, 608
 - SPI section, 608
- `mipagentstat` command
 - displaying agent status, 612-614
 - mobility agent status, 631
- MN-FAauth label, 602, 624
- mobile-foreign agent authentication, 593
- mobile-home agent authentication, 593
- Mobile IP
 - Address section
 - default mobile node, 604, 629-630
 - Network Access Identifier, 604, 628-629
 - agent advertisement, 586, 587, 591
 - agent discovery, 587-588
 - agent solicitation, 586, 587, 588
 - broadcast datagrams, 596
 - configuration file
 - Address section, 624, 626-630
 - Advertisements section, 621-623
 - General section, 621
 - GlobalSecurityParameters section, 623-624
 - Pool section, 624-625
 - SPI section, 625-626, 626, 627
 - configuration file format, 617
 - configuration file sections, 621
 - configuring, 600-604
 - datagram movement, 582
 - deploying, 599
 - deregistering, 586, 591, 592
 - displaying agent status, 612-614
 - encapsulated datagram, 584
 - encapsulation types, 595
 - functions not supported, 616
 - how it works, 584-586
 - IPsec, use of, 598
 - message authentication, 593, 597, 625
 - multicast datagram routing, 596-597
 - Network Access Identifier, 626
 - private addresses, 589-591
 - registering, 584, 586, 591
 - reverse tunnel flag, 593
 - registration messages, 591, 592, 593, 616
 - registration reply message, 594

- Mobile IP (Continued)
 - registration request, 593
 - registration request message, 594
 - reverse tunnel, 587, 589-591
 - foreign agent considerations, 594
 - home agent considerations, 594
 - multicast datagram routing, 597
 - unicast datagram routing, 596
 - RFCs not supported, 616
 - RFCs supported, 615
 - router advertisement, 616
 - sample configuration files, 617-620
 - security association, 593
 - security considerations, 597-598
 - security parameter index (SPI), 593, 625
 - state information, 632
 - unicast datagram routing, 596
 - wireless communications, 583, 588, 597
- Mobile IP topology, 582
- mobile node, 582, 583, 584, 628
 - Address section, 604
 - definition, 583
- mobility agent, 586, 594
 - Address section, 626, 627
 - configuring, 630
 - mipagent_state file, 632
 - router advertisements, 616
 - software, 615
 - status of, 631
- mobility binding, 591, 593, 594, 596
- modifying
 - DHCP macros, 342
 - DHCP options, 356
- mpathd file, 677
- multicast addresses, IPv6
 - compared to broadcast addresses, 231
 - format, 207-208
 - overview, 80
- multicast datagram routing, Mobile IP, 596-597
- multihomed hosts
 - configuring, 121-122
 - configuring during installation, 186-187
 - definition, 121
 - enabling for IPv6, 128-129
- multiple network interfaces
 - DHCP client systems, 379
 - /etc/inet/hosts file, 187
 - router configuration, 118, 120

N

- name services
 - administrative subdivisions, 64
 - database search order specification, 195, 197
 - domain name registration, 36
 - domain name system (DNS), 41, 63
 - files corresponding to network databases, 194
 - hosts database and, 187, 188
 - local files
 - description, 63
 - /etc/inet/hosts file, 185, 188
 - local files mode, 97, 98
 - network databases and, 63, 193
 - NIS, 63
 - NIS+, 63
 - nsswitch.conf file templates, 196
 - registration of DHCP clients, 308
 - selecting a service, 62, 64
 - supported services, 62
- names/naming
 - domain names
 - registration, 36
 - selecting, 63
 - top-level domains, 64
 - host name
 - administering, 62
 - /etc/inet/hosts file, 186
 - naming network entities, 62, 64
 - node name
 - local host, 106, 184
- NAT
 - configuring rules for, 540-541
 - deactivating, 552
 - limitations with IPsec, 437-438
 - NAT rules
 - appending, 562-563
 - viewing, 561-562
 - overview, 540-541
 - removing NAT rules, 562
 - using IPsec and IKE, 516-517, 518-519
 - viewing statistics, 567-568
- ndd command, viewing pfil module and, 568-569
- ndpd.conf file
 - 6to4 advertisement, 135
 - creating, on an IPv6 router, 127

- ndpd.conf file
 - interface configuration variables, 212
 - keyword list, 211-215
 - prefix configuration variables, 214
- ndpd.conf file
 - temporary address configuration, 145
- Neighbor Discovery protocol
 - address autoconfiguration, 81, 227
 - address resolution, 81
 - capabilities, 81
 - comparison to ARP, 230-232
 - duplicate address detection algorithm, 229
 - major features, 226-232
 - neighbor solicitation, 229
 - prefix discovery, 81, 228
 - router discovery, 81, 227
- neighbor solicitation, IPv6, 226
- neighbor unreachability detection
 - IPv6, 81, 229, 231
- /net/if_types.h file, 657
- netmasks database, 188
 - adding subnets, 99, 103
 - corresponding name service files, 194
 - /etc/inet/netmasks file
 - adding subnets, 99
 - editing, 191
 - router configuration, 120
 - network masks
 - applying to IPv4 address, 190
 - creating, 189, 190
 - description, 189
 - subnetting, 189
 - updating, for a router, 120
- netstat command
 - a option, 160
 - description, 157
 - displaying status of known routes, 163
 - f option, 160
 - inet option, 160
 - inet6 option, 160
 - IPv6 extensions, 221
 - Mobile IP extensions, 632
 - per-protocol statistics display, 157
 - r option, 163
 - running software checks, 178
 - syntax, 157
- Network Access Identifier
 - Mobile IP, 626
- Network Access Identifier (Continued)
 - Mobile IP Address section, 604, 628-629
- Network Address Translation (NAT), *See* NAT
- network administration
 - designing the network, 53
 - host names, 62
 - network numbers, 54
 - Simple Network Management Protocol (SNMP), 42
- network classes, 59
 - addressing scheme, 58, 59
 - class A, 202
 - class B, 203
 - class C, 203
 - IANA network number assignment, 59
 - network number administration, 54
 - range of numbers available, 59
- network client mode
 - definition, 97
 - host configuration, 106
 - overview, 98
- network clients
 - ethers database, 198
 - host configuration, 106
 - network configuration server for, 98, 104
 - systems operating as, 98
- network configuration
 - configuring
 - network clients, 105
 - services, 108
 - configuring security, 423
 - enabling IPv6 on a host, 142-147
 - host configuration modes, 97
 - IPv4 network configuration tasks, 101
 - IPv4 network topology, 99
 - IPv6-enabled multihomed hosts, 128-129
 - IPv6 router, 126
 - network configuration server setup, 104
 - router, 118
 - TCP/IP configuration modes, 99
 - configuration information, 97
 - local files mode, 98
 - network client mode, 98
 - network configuration servers, 98
- network configuration servers
 - booting protocols, 98
 - definition, 98
 - setting up, 104

- network databases, 192, 195
 - bootparams database, 197
 - corresponding name service files, 194
 - DNS boot and data files and, 193
 - ethers database
 - checking entries, 178
 - overview, 198
 - hosts database
 - checking entries, 178
 - name services, affect on, 188
 - name services, forms of, 193
 - name services affect on, 187
 - overview, 185, 188
 - name services' affect, 193, 195
 - netmasks database, 188, 194
 - networks database, 199
 - nsswitch.conf file and, 193, 195, 197
 - protocols database, 200
 - services database, 200
- network example for IPQoS, 717
- network interface, configuring, 112-118
- network interface card (NIC)
 - administering NICs not present at boot time, 651-652
 - attaching NICs with DR, 650
 - definition, 639
 - detaching NICs with DR, 651
 - dynamic reconfiguration, 641
 - failure and failover, 640
 - NIC speed in an IPMP group, 639-640
 - NICs, types of, 113
 - NICs that support IPMP, 646
 - repair detection, 640
- network interfaces
 - displaying DHCP status, 378
 - IP addresses and, 61
 - monitoring by DHCP service, 312-313
 - multiple network interfaces
 - /etc/inet/hosts file, 187
- network layer (OSI), 37
- Network Management rights profile, 467
- network numbers, 35
- network planning, 51, 67
 - adding routers, 64, 67
 - design decisions, 53
 - IP addressing scheme, 54, 61
 - name assignments, 62, 64
 - registering your network, 56
- network prefix, IPv4, 60
- network security, configuring, 423
- Network Security rights profile, 467-468
- network topologies for IPQoS, 696
 - configuration example, 711
 - LAN with IPQoS-enabled firewall, 698
 - LAN with IPQoS-enabled hosts, 697
 - LAN with IPQoS-enabled server farms, 697
- network topology, 65
 - DHCP and, 264
- networks database
 - corresponding name service files, 195
 - overview, 199
- new features
 - configuring target systems in IPMP, 663-665
 - default address selection, 173-176
 - DHCP event scripts, 386-388
 - DHCP on logical interfaces, 379
 - IKE enhancements, 483
 - inetconv command, 105
 - IPsec enhancements, 440-441
 - link-based failure detection, 646
 - manually configuring a link-local address, 147-149
 - manually configuring a MAC address, 657-659
 - routeadm command, 120, 126
 - SCTP protocol, 109-112
 - Service Management Facility (SMF), 105
 - site prefix, in IPv6, 75, 76-77
 - temporary addresses in IPv6, 144-147
- next-hop, 231
- next-hop determination, IPv6, 81
- NFS services, 42
- NIC
 - See* network interface card (NIC)
 - specifying for Solaris IP Filter, 549-550
- NIS
 - adding IPv6 address, 139
 - domain name registration, 36
 - network databases, 63, 193
 - selecting as name service, 63
- NIS+
 - and DHCP data store, 389-392
 - selecting as name service, 63
- nisaddcred command, and DHCP, 392
- nischmod command, and DHCP, 391
- nislsl command, and DHCP, 391

- nisstat command, and DHCP, 390
- node, IPv6, 73
- node name
 - local host, 106, 184
- nodename file
 - deleting for network client mode, 106
 - description, 184
- nslookup command, 243
 - IPv6, 140
- nsswitch.conf file, 195, 197
 - changing, 196, 197
 - examples, 196
 - modifications, for IPv6 support, 242-243
 - name service templates, 196
 - network client mode configuration, 106
 - syntax, 196

O

- od command, 488
- Open Systems Interconnect (OSI) Reference Model, 36, 37
 - /opt/SUNWconn/lib/libpkcs11.so entry, in ike/config file, 530

P

- p option
 - in.iked daemon, 492, 495
- packet filtering
 - activating a different rule set, 556-557
 - appending
 - rules to active set, 558
 - rules to inactive set, 559
 - configuring, 537-540
 - deactivating, 551
 - managing rule sets, 555-561
 - removing
 - active rule set, 557-558
 - inactive rule set, 560-561
 - specifying a NIC, 549-550
 - switching between rule sets, 559-560
- packet flow
 - relay router, 240
 - through tunnel, 239

- packet flow, IPv6
 - 6to4 and native IPv6, 240
 - through 6to4 tunnel, 239
- packets
 - checking flow, 170
 - data encapsulation, 44, 45
 - description, 43
 - displaying contents, 170
 - dropped or lost, 39, 164
 - fragmentation, 38
 - header
 - IP header, 46
 - TCP protocol functions, 39
 - IP protocol functions, 38
 - IPv6 header format, 208-210
 - life cycle, 44, 47
 - application layer, 44
 - data-link layer, 46
 - Internet layer, 45
 - physical network layer, 46
 - receiving host process, 46, 47
 - transport layer, 44, 45
 - protecting
 - inbound packets, 428
 - outbound packets, 428
 - with IKE, 479
 - with IPsec, 428, 432-434
 - transfer
 - router, 66, 67
 - TCP/IP stack, 43, 47
 - UDP, 45
 - verifying protection, 465-467
- params clause
 - defining global statistics, 721, 773
 - for a flowacct action, 727
 - for a marker action, 725
 - for a metering action, 738
 - syntax, 773
- per-hop behavior (PHB), 692
 - AF forwarding, 692
 - defining, in the IPQoS configuration file, 740
 - EF forwarding, 692
 - using, with dscpmk marker, 763
- perfect forward secrecy (PFS)
 - description, 478
 - IKE, 478
- PF_KEY socket interface
 - IPsec, 431, 439

- pfil module, 542
 - viewing statistics, 568-569
- PFS, *See* perfect forward secrecy (PFS)
- physical interface
 - adding, after installation, 113
 - configuring, 112-118
 - definition, 112, 639
 - failure detection, 646
 - network interface card (NIC), 113
 - removing, 115
 - repair detection with IPMP, 648
 - VLANs, definition, 115-118
- physical layer (OSI), 37
- physical network layer (TCP/IP), 38, 46
- ping command, 165
 - description, 164
 - extensions for IPv6, 222
 - running, 165
 - s option, 164
 - syntax, 164
- PKCS #11 library
 - in ike/config file, 530
 - specifying path to, 531
 - using with hardware for IKE, 522
- pkcs11_path keyword
 - description, 530
 - IKE configuration file, 522
 - ikecert command and, 531
 - using, 506, 521
- pntadm command
 - description, 256, 409
 - examples, 324
 - using in scripts, 410
- policies, IPsec, 434-435
- policy files
 - ike/config file, 440, 482, 528
 - ipsecinit.conf file, 470-471
 - ipsecpolicy.conf temporary file, 469
 - security considerations, 471
- Pool label, 604, 609, 628, 629
- Pool section
 - labels and values, 625
 - Mobile IP configuration file, 624-625
- ports, TCP, UDP, and SCTP port numbers, 200
- PPP links
 - troubleshooting
 - packet flow, 170
- prefix
 - network, IPv4, 60
 - site prefix, IPv6, 76-77
 - subnet prefix, IPv6, 77
- prefix discovery, in IPv6, 81
- prefixes
 - router advertisement, 228, 231, 233
- PrefixFlags label, 602, 622
- presentation layer (OSI), 36
- preshared keys (IKE)
 - description, 480
 - storing, 529
 - task map, 486
- preshared keys (IPsec)
 - creating, 461-465
 - replacing, 490
- primary network interface, 113
- private addresses, Mobile IP, 589-591
- private keys, storing (IKE), 530
- privilege level
 - checking in IKE, 490, 495
 - setting in IKE, 492, 495
- probe-based failure detection
 - configuring target systems, 663-665
 - definition, 647
 - failure detection time, 647
 - probe traffic, IPMP, 642
 - probing targets, 647
- probing targets, in .mpathd daemon, 642
- protecting
 - IPsec traffic, 425
 - keys in hardware, 481
 - mobile systems with IPsec, 513-520
 - packets between two systems, 445
 - VPNs with IPsec, 450-456
 - web server with IPsec, 447-449
- protection mechanisms, IPsec, 432-434
- protocol layers
 - OSI Reference Model, 36, 37
 - packet life cycle, 44, 47
 - TCP/IP protocol architecture model, 37, 42
 - application layer, 37, 40, 42
 - data-link layer, 37, 38
 - Internet layer, 37, 38
 - physical network layer, 37, 38
 - transport layer, 37, 39
- protocol statistics display, 157

- protocols database
 - corresponding name service files, 194
 - overview, 200
- proxy keyword, IKE configuration file, 511
- public key certificates, *See* certificates
- public keys, storing (IKE), 532
- public topology, IPv6, 78
- publickeys database, 532

Q

- q option, in `routed` daemon, 201
- QoS policy, 685
 - creating filters, 704
 - implementing, in the IPQoS configuration file, 715
 - planning task map, 700
 - template for policy organization, 699
- quality of service (QoS)
 - QoS policy, 684
 - tasks, 681

R

- random numbers, generating with `od` command, 488
- RARP protocol
 - checking Ethernet addresses, 178
 - description, 98
 - Ethernet address mapping, 198
 - RARP server configuration, 104
- RBAC
 - and DHCP commands, 256
 - IPsec and, 444
- RDISC
 - description, 42, 201
- receiving hosts
 - packet travel through, 46, 47
- Reconfiguration Coordination Manager (RCM)
 - framework, 651
- redirect
 - IPv6, 81, 226, 231
- refreshing
 - See* replacing
 - preshared keys (IPsec), 490

- registering
 - domain names, 36
 - networks, 56
- registration
 - messages, 591, 594
 - Mobile IP, 584, 586, 591
 - reply message, 594
 - request, 593
 - reverse tunnel flag, 593
- RegLifetime label, 602, 622
- relay router, 6to4 tunnel configuration, 136, 137
- repair detection, with IPMP, 640, 648
- replacing
 - IPsec SAs, 462
 - manual keys (IPsec), 462
 - preshared keys (IPsec), 490
- ReplayMethod label, 603, 626
- Requests for Comments (RFCs), 48
 - definition, 48
 - IKE, 427
 - IPQoS, 683
 - IPsec, 427
 - IPv6, 71
- requirements for IPMP, 641
- retry_limit keyword, IKE configuration file, 524
- retry_timer_init keyword, IKE configuration file, 524
- retry_timer_max keyword, IKE configuration file, 524
- reverse tunnel
 - foreign agent considerations, 594
 - home agent considerations, 594
 - Mobile IP, 587, 589-591
 - multicast datagram routing, 597
 - unicast datagram routing, 596
- reverse zone file, 138
- ReverseTunnel label, 602, 622
- ReverseTunnelRequired label, 602, 623
- rights profiles
 - Network Management, 467
 - Network Security, 467
- rlogin command, packet process, 44
- roles, creating network security role, 467-468
- route command
 - inet6 option, 222
 - IPsec, 455, 459

- routeadm
 - IP forwarding, 129
 - IPv4 router configuration, 120
- routeadm command
 - configuring VPN with IPsec, 456
 - enabling dynamic routing, 107
 - IP forwarding, 120, 452
 - IPv6 router configuration, 126
 - multihomed hosts, 122
 - turning on dynamic routing, 121
- router advertisement
 - IPv6, 226, 227, 230, 232-233
 - Mobile IP, 616
 - prefix, 228
- router discovery, in IPv6, 81, 222, 227, 230
- router solicitation
 - IPv6, 226, 228
- routers
 - adding, 64, 67
 - addresses for DHCP clients, 270
 - configuring, 201
 - for IPv4 networks, 118
 - IPv6, 126
 - network interfaces, 120
 - default address, 102
 - definition, 118, 201
 - dynamic routing, 107
 - /etc/defaultrouter file, 185
 - local files mode configuration, 103
 - network topology, 65
 - packet transfer, 66, 67
 - problems upgrading for IPv6, 179
 - role, in 6to4 topology, 238
 - routing protocols
 - automatic selection, 120
 - description, 42, 201, 202
 - static routing, 107
- routing, IPv6, 232
- routing information protocol (RIP)
 - description, 42, 201
- routing protocols
 - automatic selection, 120
 - description, 42, 201, 202
 - RDISC
 - description, 42, 201
 - RIP
 - description, 42, 201

- routing tables
 - description, 66
 - displaying, 177
 - in .routed daemon creation of, 201
 - packet transfer example, 67
 - space-saving mode, 201
 - subnetting and, 189
 - tracing all routes, 169-170
- rpc.bootparamd daemon, 98
- RSA encryption algorithm, 531
- rule sets
 - See See Solaris IP Filter
 - inactive
 - See also Solaris IP Filter
 - NAT, 540-541
 - packet filtering, 537-542

S

- S option, in .routed daemon, 201
- s option, ping command, 165
- SCTP protocol
 - adding SCTP-enabled services, 109-112
 - description, 40
 - displaying statistics, 157
 - displaying status, 159
 - IPsec and, 444
 - limitations with IPsec, 438
 - service in /etc/inet/services file, 200
- security
 - IKE, 527
 - IPsec, 425
- security associations, Mobile IP, 593
- security associations (SAs)
 - adding IPsec, 446
 - creating manually, 461-465
 - flushing IPsec SAs, 462
 - getting keys for, 460-461
 - IKE, 527
 - IPsec, 431-432, 446
 - IPsec database, 472
 - ISAKMP, 479
 - random number generation, 479
 - replacing IPsec SAs, 462
- security associations database (SADB), 472
- security considerations
 - 6to4 relay router issues, 180

- security considerations (Continued)
 - authentication header (AH), 433
 - configuring
 - IKE to find hardware, 506
 - IKE transmission parameters, 524
 - IKE with certificates, 497
 - IKE with preshared keys, 487
 - IPsec, 445
 - encapsulating security payload (ESP), 433
 - ike/config file, 528
 - ipseccomp command, 471
 - ipseccinit.conf file, 471
 - ipseckey command, 473
 - ipseckey file, 465
 - IPv6-enabled networks, 92
 - latched sockets, 471
 - Mobile IP, 597-598
 - preshared keys, 480
 - security protocols, 433
- security parameter index (SPI)
 - constructing, 461
 - description, 431-432
 - key size, 461
 - Mobile IP, 593, 625
- security policy
 - ike/config file (IKE), 440
 - IPsec, 434-435
 - ipseccinit.conf file (IPsec), 446, 470-471
- security policy database (SPD)
 - configuring, 469
 - IPsec, 426, 427
- security protocols
 - authentication header (AH), 432
 - encapsulating security payload (ESP), 432-433
 - IPsec protection mechanisms, 432
 - overview, 426
 - security considerations, 433
- selectors, 688
 - IPQoS 5-tuple, 687
 - planning, in the QoS policy, 704
 - selectors, list of, 758
- sending hosts
 - packet travel through, 44, 46
- servers, IPv6
 - enabling IPv6, 147-149
 - planning tasks, 90
- service-level agreement (SLA), 684
- service-level agreement (SLA) (Continued)
 - billing clients, based on flow accounting, 752
 - classes of services, 687
 - providing different classes of service, 686
- services
 - network and svcadm command, 453, 457
- services database
 - corresponding name service files, 194
 - overview, 200
 - updating, for SCTP, 109
- session layer (OSI), 36
- Simple Network Management Protocol (SNMP), 42
- site-local addresses, IPv6, 83
- site prefix, IPv6
 - advertising, on the router, 127
 - definition, 75, 76
 - how to obtain, 93
- site topology, IPv6, 78
- Size label, 603, 625
- slots, in hardware, 532
- SNMP (Simple Network Management Protocol), 42
- snoop command
 - checking packet flow, 170
 - checking packets between server and client, 172
 - displaying packet contents, 170
 - extensions for IPv6, 221
 - ip6 protocol keyword, 221
 - Mobile IP extensions, 633
 - monitoring DHCP traffic, 397
 - sample output, 402
 - monitoring IPv6 traffic, 173
 - verifying packet protection, 465-467
 - viewing protected packets, 475
- sockets
 - displaying socket status with netstat, 160
 - IPsec security, 471
 - security considerations, 447
- Solaris cryptographic framework, IPsec, and, 472
- Solaris IP Filter
 - address pools
 - appending, 564-565
 - removing, 564
 - viewing, 563-564
 - address pools and, 541-542

- Solaris IP Filter (Continued)
 - configuration file examples, 536-537
 - creating configuration files, 572-573
 - deactivating, 554
 - NAT, 552
 - on a NIC, 552-554
 - enabling, 546-548
 - /etc/ipf/ipf.conf file, 572-573
 - /etc/ipf/ipnat.conf file, 572-573
 - /etc/ipf/ippool.conf file, 572-573
 - flush log file, 570-571
 - guidelines for using, 536
 - ifconfig command, 536
 - ipf command, 548-549
 - ipf.conf file, 537-540
 - ipnat command, 548-549
 - ipnat.conf file, 540-541
 - ippool command, 563-564
 - ippool.conf file, 541-542
 - managing packet filtering rule sets, 555-561
 - NAT and, 540-541
 - NAT rules
 - appending, 562-563
 - viewing, 561-562
 - open source information, 536
 - overview, 535-536
 - packet filtering overview, 537-540
 - pfil module, 542
 - re-enabling, 548-549
 - removing
 - NAT rules, 562
 - rule set
 - activating different, 556-557
 - rule sets
 - active, 556
 - appending to active, 558
 - appending to inactive, 559
 - inactive, 556
 - removing, 557-558
 - removing inactive, 560-561
 - switching between, 559-560
 - rule sets and, 537-542
 - saving logged packets to a file, 571
 - specifying a NIC, 549-550
 - viewing
 - address pool statistics, 568
 - log files, 569-570
 - NAT statistics, 567-568
- Solaris IP Filter, viewing (Continued)
 - pfil statistics, 568-569
 - state statistics, 567
 - state tables, 566-567
 - space-saving mode, in .routed daemon
 - option, 201
 - SPI label, 608, 627, 628, 629
 - SPI section
 - labels and values, 625
 - Mobile IP configuration file, 625-626, 626, 627
 - standby interface
 - configuring for an IPMP group, 665-667
 - configuring test address on, 666
 - definition, 644-645
 - standby parameter
 - ifconfig command, 645, 666
 - state information, Mobile IP, 632
 - state statistics, viewing, 567
 - state tables, viewing, 566-567
 - stateless address autoconfiguration, 228
 - static routing, 107, 185
 - statistics
 - packet transmission (ping), 164, 165
 - per-protocol (netstat), 157
 - statistics for IPQoS
 - enabling class-based statistics, 773
 - enabling global statistics, 721, 773
 - generating, through the kstat command, 754
 - storing
 - IKE keys on disk, 502, 532
 - IKE keys on hardware, 481, 522-523
 - subdivisions, administrative, 64
 - subnet prefix, IPv6, 77
 - subnets
 - IPv4
 - addresses and, 189
 - netmask configuration, 103
 - IPv4 addresses and, 190
 - IPv6
 - 6to4 topology and, 238
 - definition, 74
 - suggestions for numbering, 93-94
 - netmasks database, 188
 - editing /etc/inet/netmasks file, 191
 - network mask creation, 189, 190
 - network configuration servers, 98

- subnets (Continued)
 - network masks
 - applying to IPv4 address, 190
 - creating, 190
 - overview, 189
 - subnet number, IPv4, 189
 - subnet number in IPv4 addresses, 59
 - subnet prefix, IPv6, 77
- Sun Crypto Accelerator 1000 board, 481
 - using with IKE, 521-522
- Sun Crypto Accelerator 4000 board
 - accelerating IKE computations, 481
 - storing IKE keys, 481
 - using with IKE, 522-523
- svcadm command
 - disabling network services, 453, 457
- symbolic names for network numbers, 191
- SYN segment, 45
- sys-unconfig command
 - and DHCP client, 376
- syslog.conf file logging for IPQoS, 746
- systems, protecting communication, 445

T

- t option
 - ikecert certlocal command, 497
 - ikecert command, 531
 - inetd daemon, 108
- T option
 - ikecert command, 506, 531, 532
- target system, in IPMP
 - configuring, in a shell script, 664-665
 - configuring manually, 663-664
 - definition, 640
- task map
 - IPQoS
 - configuration planning, 695
- task maps
 - accelerating IKE keys on hardware, 520
 - Changing IKE Transmission Parameters, 523
 - Configuring IKE for Mobile Systems, 512
 - configuring IKE to find attached hardware, 520
 - configuring IKE with public key certificates, 496

- task maps (Continued)
 - DHCP
 - IP address management decisions, 271
 - making decisions for DHCP server configuration, 268
 - modifying DHCP service options, 299
 - moving DHCP server configuration data, 366
 - preparing network for DHCP, 264
 - supporting BOOTP clients, 321
 - supporting information-only clients, 362
 - supporting remove boot and diskless clients with DHCP, 361
 - working with DHCP macros, 340
 - working with DHCP networks, 311
 - working with DHCP options, 350
 - working with IP addresses, 324
 - IKE, 485
 - IKE for mobile systems, 512
 - IKE with customized transmission parameters, 523
 - IKE with hardware, 520
 - IKE with preshared keys, 486
 - IKE with public key certificates, 496
 - IPMP
 - dynamic reconfiguration (DR) administration, 655
 - IPMP group configuration, 654-655
 - IPQoS
 - configuration file creation, 715
 - flow-accounting setup, 751
 - QoS policy planning, 700
 - IPsec, 443
 - IPv4 network
 - adding subnets, 99-101
 - IPv6
 - configuration, 123-124
 - planning, 85-86
 - tunnel configuration, 129-130
 - Mobile IP
 - configuration, 599-600
 - modifying a configuration, 605-606
 - network administration tasks, 152-153
 - network configuration, 96
 - storing IKE keys on hardware, 520
- TCP/IP networks
 - configuration files, 183
 - /etc/defaultdomain file, 185

- TCP/IP networks, configuration files (Continued)
 - /etc/defaultrouter file, 185
 - /etc/hostname.interface file, 184
 - /etc/nodename file, 106, 184
 - hosts database, 185, 188
 - netmasks database, 188
- configuring
 - host configuration modes, 97, 99
 - local files mode, 104
 - network clients, 105
 - network configuration server setup, 104
 - network databases, 192, 195, 197
 - nsswitch.conf file, 195, 197
 - prerequisites, 96
 - standard TCP/IP services, 108
- host configuration modes, 97, 99
 - local files mode, 97, 98
 - mixed configurations, 98
 - network client mode, 98
 - network configuration servers, 98
 - sample network, 99
- IPv4 network configuration tasks, 101
- IPv4 network topology, 99
- network numbers, 35
- protecting with ESP, 432
- troubleshooting, 172
 - displaying packet contents, 170
 - general methods, 177
 - ifconfig command, 153
 - netstat command, 157
 - packet loss, 164, 165
 - ping command, 164, 165
 - software checks, 177
 - third-party diagnostic programs, 177
- TCP/IP protocol suite, 35
 - data communications, 43, 47
 - data encapsulation, 43, 47
 - displaying statistics, 157
 - dual-stack protocols, 88
 - further information, 47
 - books, 47
 - FYIs, 48
 - internal trace support, 47
 - OSI Reference Model, 36, 37
 - overview, 35, 36
 - standard services, 108
 - TCP/IP protocol architecture model, 37, 42
- TCP/IP protocol suite, TCP/IP protocol architecture model (Continued)
 - application layer, 37, 40, 42
 - data-link layer, 37, 38
 - Internet layer, 37, 38
 - physical network layer, 37, 38
 - transport layer, 37, 39
- TCP protocol
 - description, 39
 - displaying statistics, 157
 - establishing a connection, 45
 - segmentation, 45
 - services in /etc/inet/services file, 200
- TCP wrappers, enabling, 112
- Telnet protocol, 41
- temporary address, in IPv6
 - configuring, 144-147
 - definition, 144-147
- test addresses, IPMP
 - configuring
 - IPv4, 659
 - IPv6, 660
 - on a standby interface, 666
 - definition, 642
 - IPv4 requirements, 643
 - IPv6 requirements, 643
 - preventing use by applications, 644
 - probe traffic and, 642
 - standby interface, 645
- test parameter, ifconfig command, 659
- tftp protocol
 - description, 41
 - network configuration server booting protocol, 98
- /tftpboot directory creation, 104
- three-way handshake, 45
- timestamps, 603, 623
- token ID, in hardware, 532
- Token ring, IPMP support for, 657
- tokenmt meter, 688
 - color-awareness configuration, 689, 761
 - metering rates, 760
 - rate parameters, 761
 - single-rate meter, 761
 - two rate-meter, 761
- tokens argument, ikecert command, 530
- topology, 65

- tracert command
 - definition, 168-170
 - extensions for IPv6, 222
 - tracing routes, 169-170
- traffic conformance
 - defining, 738
 - outcomes, 688, 760
 - planning
 - outcomes in the QoS policy, 707
 - rates in the QoS policy, 706
 - rate parameters, 760, 761
- traffic management
 - controlling flow, 688
 - forwarding traffic, 691, 692, 693
 - planning network topologies, 697
 - prioritizing traffic flows, 686
 - regulating bandwidth, 685
- transition to IPv6, 6to4 mechanism, 237
- transmission parameters
 - IKE global parameters, 524
 - IKE tuning, 524-526
- transmission parameters (IKE), task map, 523
- transport layer
 - data encapsulation, 44, 45
 - obtaining transport protocol status, 159-160
 - OSI, 36
 - packet life cycle
 - receiving host, 46
 - sending host, 44, 45
 - TCP/IP
 - description, 37, 39
 - SCTP protocol, 40, 109-112
 - TCP protocol, 39
 - UDP protocol, 40
- transport mode, IPsec, 435-436
- Triple-DES encryption algorithm, IPsec
 - and, 434
- troubleshooting
 - checking PPP links
 - packet flow, 170
 - DHCP, 389
 - IKE payload, 506
 - IKE transmission timing, 524-526
 - IPv6 problems, 179-181
 - TCP/IP networks
 - checking packets between client and server, 172
- troubleshooting, TCP/IP networks (Continued)
 - displaying interface status with
 - ifconfig command, 153, 155-156
 - displaying status of known routes, 163
 - general methods, 177
 - monitoring network status with netstat
 - command, 157
 - monitoring packet transfer with snoop
 - command, 170
 - observing transmissions from
 - interfaces, 160
 - obtaining per-protocol statistics, 157-158
 - obtaining transport protocol
 - status, 159-160
 - packet loss, 164, 165
 - ping command, 165
 - probing remote hosts with ping
 - command, 164
 - software checks, 177
 - third-party diagnostic programs, 177
 - tracert command, 168-170
 - tracing in.ndpd activity, 167-168
 - tracing in.routed activity, 166-167
- tswtclmt meter, 688, 762
 - metering rates, 762
- tun module, 235
- tunnel mode, IPsec, 435-436
- tunneling, 584, 595, 598
- tunnels
 - 6to4
 - known problems, 180
 - 6to4 tunnel packet flow, 239
 - 6to4 tunnel topology, 238
 - configuring IPv6
 - 6to4, to a 6to4 relay router, 136
 - 6to4 tunnels, 133
 - examples, 220
 - IPv4 over IPv6, 132
 - IPv6 over IPv4, 130-131
 - IPv6 over IPv6, 131
 - ifconfig security options, 474-475
 - IPsec, 436
 - IPv6, automatic, 237
 - IPv6, manually configured, 235-237
 - IPv6 tunneling mechanisms, 233
 - planning, for IPv6, 91-92
 - protecting packets, 436
 - topology, to 6to4 relay router, 240

turning on
 an IPv6-enabled network, 123-124
 network configuration daemons, 104
Type label, 609, 626, 628, 629

U

UDP protocol
 description, 40
 displaying statistics, 157
 services in `/etc/inet/services` file, 200
 UDP packet process, 45
unicast datagram routing, Mobile IP, 596
uniform resource indicator (URI), for accessing
 CRLs, 510
UNIX “r” commands, 41
unusable DHCP address, 328, 334
use_http keyword, IKE configuration file, 511
user priority value, 689
`/usr/sbin/6to4relay` command, 137
`/usr/sbin/in.rdisc` program,
 description, 202
`/usr/sbin/in.routed` daemon
 description, 201
 space-saving mode, 201
`/usr/sbin/inetd` daemon
 checking the status of `inetd`, 178
 services started by, 108
`/usr/sbin/ping` command, 165
 description, 164
 running, 165
 syntax, 164

V

-V option, snoop command, 475
`/var/inet/ndpd_state.interface`
 file, 223
verifying, packet protection, 465-467
Version label, 602, 621
viewing, IPsec policy, 449
virtual LAN (VLAN) devices on an IPQoS
 network, 765
virtual private networks (VPN)
 configuring with `routedadm` command, 452,
 456

virtual private networks (VPN) (Continued)
 constructed with IPsec, 437
 IPv4 example, 450
 IPv6 example, 456
 protecting with IPsec, 450-456
visitor list
 foreign agent, 612
 Mobile IP, 631
VLAN
 configuration, 116-118
 definition, 115-118
 ID, 116
 naming format, 117
 virtual device, 117
VPN, *See* virtual private networks (VPN)

W

web servers
 configuring for IPQoS, 718, 719, 728, 729
 protecting with IPsec, 447-449
wide area network (WAN)
 Internet
 domain name registration, 36
wildcards in `bootparams` database, 198
wireless communications
 Mobile IP, 583, 588, 597
wrappers, TCP, 112

Z

zone file, 138
zones
 IPsec and, 439, 444
 key management and, 444

