Directory-Enabled Networking

Directory services are the cornerstone for creating intelligent networks. A directory service is a physically distributed, logically centralized repository of infrequently changing data that is used to manage the entire enterprise networking environment. Today, the computing environment that must be managed includes not only the computers themselves, but also the network devices that connect them. Extending networks to include directory services is a response to the new, more demanding requirements for network management by means of the directory.

A traditional directory service provides a means for locating and identifying users and available resources in a distributed system. Directory services also provide the foundation for adding, modifying, removing, renaming, and managing system components without disrupting the services provided by other system components. Today's directory services are used to do the following:

- Store information about system components in a distributed manner. The directory is replicated among several servers so that a user or service needing access to the directory can query a local server for the information.
- Support white pages (by attribute, such as name, for example, "find the phone number for James Smith") and yellow pages (by classification, for example, "find all color printers on the third floor") lookup.
- Allow single-user logon to services, resources, and applications.
- Enable a location-independent point of administration and management. Note that administrative tools do not have to be centrally located and managed.
- Replicate data to provide consistent access. Modifications made to any replica of the directory are propagated around the network so that any application accessing the directory anywhere sees consistent information after the change is propagated.

Rapid Internet growth over the past several years has created the need for more robust, scalable, and secure directory services. As PCs become more powerful, people are finding more ways to fully utilize the power of their computers. Residential customers desire rich multimedia services, such as data and video. Corporate customers are looking to telcos and service providers for powerful, yet affordable, services. Users want a reliable, easy-to-use, friendly service.

A fundamental shift toward bandwidth-intensive and isochronous network applications is occurring. Current directory services technology is not designed to meet the ever-increasing demands of today's public and private network applications because current directory services were built mainly to accommodate administrative needs. The directory must be transformed from a "dumb warehouse" to an authoritative, distributed, intelligent repository of information for services and applications. The directory is the foundation for an intelligent infrastructure. Bandwidth-intensive and isochronous network applications require that the devices that lie on a path through the network between source and end device be configured appropriately if they are to function properly. This configuration is often dynamic, taking place on demand when a particular user logs on to the network from any of a number of possible locations. Only when management information about the users, network devices, and services involved is available in a single, authoritative location is it possible to actually manage this new class of applications.

The Purpose and Scope of Directory-Enabled Networking

This section defines the problem domains, information model, usage, and detailed directory schema for integrating networks with directory services. Cisco Systems and Microsoft Corporation have introduced an initiative to define a rational, usable model for enhancing networks via integration with the directory service. In these networks, the network resources (devices, operating systems, management tools, and applications) use the directory service to do the following:

- Publish information about themselves
- Discover other resources
- Obtain information about other resources

The directory service becomes the hub around which the distributed system turns; the degree of cooperation among network components and distributed applications is dramatically enhanced. The result is a network in which service to users is predictable and repeatable, security is strengthened, and management is easier.

This section defines an environment for directory-enabled networks. The environment defined here provides the basis for network equipment vendors, directory service providers, software developers, common carriers, and end users to develop the interoperating components that will comprise next-generation networks.

Networks, the Universe, and You

Administrative needs and the tools that service them have evolved as distributed systems have evolved. Today’s directory services were designed to provide central management of security and contact information in a network with a relatively small number of relatively large computers. Network management has been the province of more specialized tools, each with its own information store. Application management has been addressed as an afterthought, when it has been addressed at all.

Convergence of the information stores holding the universe of management information has been difficult. The result is an environment in which vertical management tools have proliferated. Lack of integration and the sheer complexity of the tools themselves has become a barrier to the deployment of new applications.

Administrators need a level of control over their networks that is currently unavailable. Streaming multimedia, use of public networks and the attendant security concerns, and rapidly growing user communities present a tremendous challenge.

Simply managing individual devices is no longer sufficient. Network administrators need to define and manage *policies* to control the network and its resources in a distributed, yet logically centralized, manner. In general terms, policies define what resources a given consumer can use in the context of a given application or service. Inability to easily manage policies is a significant barrier to deployment of leading-edge distributed applications.

Note A *consumer* is a user, an application, a service, or another user of resources.

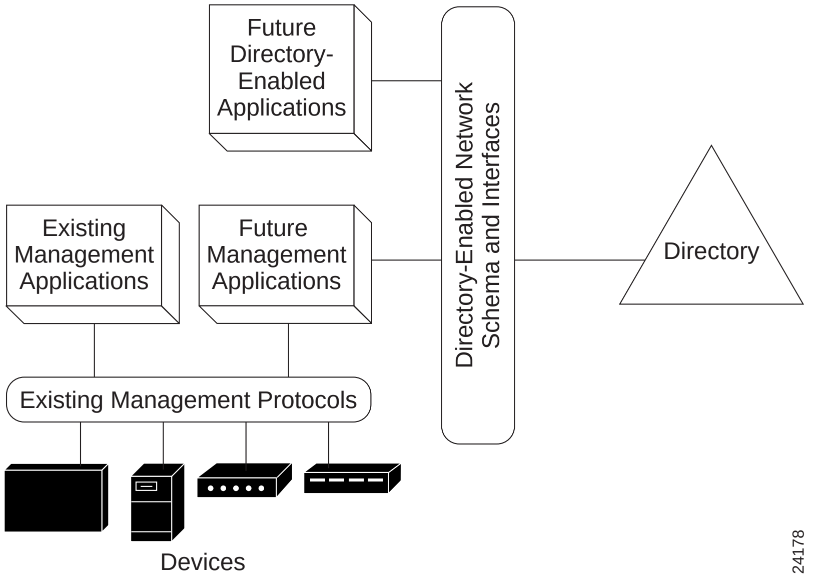
Defining and managing policies requires a common store of well-defined information about the network and its resources—users, applications, devices, protocols, and media—and the relationships among these elements. This is information *about the network* as well as the information traditionally viewed as defining the network (for example, routing tables). At issue is where to store policy and other information that needs to be applied across components in a way that makes it usable by a broad range of consumers.

A scalable, secure directory service that presents a logically centralized view of physically distributed information is the logical place to store the meta-information essential to creating and managing a next-generation network. The specification for the integration of directory services and network services defines the information model and schema to make this possible.

Directory Service and Network Management

Network elements typically have a dynamic state and a persistent state. Dynamic state is well addressed by network management protocols. However, there is no standard way to describe and store persistent state. Moreover, existing tools and applications focus on managing individual network elements rather than the entire network. This specification defines a standard schema for storing persistent state *and* an information model for describing the relationships among objects representing users, applications, network elements, and network services (see Figure 48-1). Network management protocols (such as SNMP, CMIP, and HMMP) are used to talk *to* the network elements. The network schema extensions for the directory service are used to talk *about* network elements.

Figure 48-1 This figure displays a high-level overview of the directory-enabled network schema.


Future Directory-Enabled Applications
Existing Management Applications
Future Management Applications
Directory-Enabled Network Schema and Interfaces
Directory
Existing Management Protocols
Devices
24178

The integration of the network infrastructure with the directory service allows the applications and users to discover the existence of devices and relationships by querying the directory service, rather than contacting the individual devices and aggregating the results. Exposing network elements in the directory enhances manageability and usability while reducing the load on the network. The end user and administrator experience is enhanced because there is a single, authoritative place to obtain the information of interest.

The Common Information Model (CIM)

CIM is an object-oriented conceptual model for the information required to manage many common aspects of complex computer systems, defined by the Desktop Management Task Force (DMTF).

Ongoing development of CIM is part of an industry-wide initiative for enabling enterprise management of devices and applications. A primary goal of CIM is the presentation of a consistent view of the managed environment, independent of the various protocols and data formats supported by those devices and applications. Many network infrastructure and management software providers have accepted CIM as an information model for enterprise management tools.

The schema for network integration defined in this specification and CIM are complementary. The extended schema is primarily concerned with the expression and management of policy in both enterprise and service provider networks. CIM is primarily concerned with the management of individual components in the context of the enterprise. The enhanced, integrated network and directory service and CIM have many information needs in common.

The schema for integrating networks and the directory service incorporates concepts from both X.500 and CIM. The use of CIM promotes synergy between integrated, enhanced network and directory applications and management applications that use CIM:

- CIM and applications written to use CIM are natural sources of information for the directory.
- The directory is a natural source of information for CIM and applications written to use CIM, and it adds models for defining and enforcing policy.
- Network applications integrated with the directory benefit from CIM, and CIM applications benefit from network applications integrated with the directory, with minimal effort on the application developer’s part because the directory-enabled network schema is an extension of the CIM schema. Thus, there is no need for cumbersome information mapping.

The Extended Schema and Other Device Schemata

Schemata defined by SNMP (MIBs), DMTF CIM, and so on are intended primarily to address the details of individual devices. The intent of the integrated, extended schema is to leverage the information exposed by existing schemata and management frameworks, not to replace them.

This specification exposes network element information and relationships gathered from the network with existing protocols and schemata using the widely available and well-understood protocol Lightweight Directory Access Protocol (LDAP), without imposing LDAP on the devices themselves.

Network Applications Integrated with the Directory and Other Network Protocols

The schema and information model defined augments existing network services and associated protocols, such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and RADIUS.

The directory provides a common store for network information; the information model describes the relationships that can be represented in the directory. The usage model defines how existing network services and protocols work with the elements in the information model to accomplish specific goals, such as coordinating IP address allocation across multiple DHCP servers, establishing and propagating remote access login policy, and so on.

Deliverables

A set of specifications in a vacuum is not helpful in building actual products. Completeness requires one or more implementations illustrating the use and deployment of the information model and detailed schema defined by this specification.

Deliverables in the Near Term

The participants in the open process will deliver an integrated network and directory environment consisting of the following:

- Abstractions of the eight major network objects—device, protocol, media, service, application, profile, policy, and user—with additional subsidiary classes as needed refined into a set of abstract classes in a schema that addresses a well-defined set of problem domains
- A usage model for the schema within the selected problem domains
- Vendor-specific products based on the foundation schema and information model described in this document

Deliverables in the Longer Term

The longer-term deliverables are a rich set of interoperable products and tools based on the schema and usage models, refined through an open process of industry review and the evolving needs of network consumers.

The Directory-Enabled Networking Vision

The vision for enhancing networking through integration with the directory service is to provide network-enabled applications with appropriate information from the directory. Eventually, intelligent network applications will transparently leverage the network on behalf of the user. The development of intelligent networks can be achieved through the following steps:

1. Relying on a robust directory service
2. Adding a standards-based schema for modeling network elements and services
3. Adding protocols for accessing, managing, and manipulating directory information

The goal of work in developing directory-enabled networks is to do the following:

- Provide support for applications that have the ability to leverage the network infrastructure transparently on behalf of the end user
- Provide a robust, extensible foundation for building network-centric applications
- Enable end-to-end network services on a per-user basis
- Enable networkwide service creation and provisioning
- Enable networkwide management

The focus is on providing management of the network as a system, not a set of disparate components. Using directory services to define the relationship among components allows the network manager to manage the network as a system. Vendors have adopted de facto and open industry standards to tie these services into its enterprise management systems. Key standards include DNS, DHCP, and LDAP. DNS and DHCP provide a critical foundation for tying system names, IP addresses, users, systems, and other services together in a more seamless and easily managed fashion. LDAP provides access to information about systems, users, services, and resources from a wide variety of vendors' network directories in an industry-standard fashion.