Sun Certified Network Administrator for Solaris 10 OS (CX-310-302)

The Sun Certified Network Administrator for the Solaris 10 Operating System exam is for candidates with three or more years of experience administering Sun systems in a networked environment/working in a network capacity. A test candidate must already be a Sun Certified System Administrator to qualify to take this examination. This certification exam tests the candidate has an in-depth knowledge of network administration skills, such as those covered in the SA-300-S10 courseware. The examination includes multiple-choice, scenario-based questions, drag-and-drop questions, and requires extensive knowledge on Solaris network administration topics including how to configure and manage the Network interface layer, the network (Internet and Transport layers), network applications, and the Solaris IP Filter.

Testing Objectives:

Section 1: Configure the Network Interface Layer

- 1.1 Explain network model fundamentals (network protocols and advantages of a layered model), layers of the TCP/IP model (Network interface, Internet, Transport, and Application), and peer-to-peer communication.
- 1.2 Explain network topologies (BUS, STAR, RING, VLAN), LAN media (IEEE identifiers and IEEE 802.3 types), and network devices (shared hubs, bridges, and switches)
- 1.3 Explain Ethernet concepts (CSMA/CD access method, difference between full-duplex and half-duplex, Ethernet statistics, and Ethernet frames, including Ethernet addresses, Ethernet address types, local Ethernet address, Ethernet-II frame, Ethernet frame encapsulation, maximum transfer unit, and Ethernet frame errors)
- 1.4 Use network utilities like snoop, netstat, and ndd to configure and troubleshoot network interfaces.
- 1.5 Examine and manage ARP and RARP, including the ARP table, in.rarpd and the hosts and ethers databases.

Section 2: Configure the Network (Internet and Transport layers)

- 2.1 Explain Internet layer protocols, IP datagrams, IP address types (unicast, broadcast, and multicast), configure netmasks for subnetting and VLSM, manage interface configuration files and configure/unconfigure logical interfaces.
- 2.2 Explain how to increase throughput and availability and given a scenario, implement and troubleshoot multipathing through the use of both configuration files and the command line.
- 2.3 Distinguish between direct routes, indirect routes, route table populations (static, default, and dynamic), explain routing protocols (interior and exterior gateway), and routing tables (entries, flags, search order, host route, network route, and default route.)
- 2.4 Configure a static route (/etc/defaultrouter, /etc/gateways and manual) and explain router discovery protocol (RDISC).
- 2.5 Distinguish between the procedures associated with dynamic routing for both RIP versions 1 and 2 and manage the in.routed daemon and explain the operation of CIDR.
- 2.6 Configure boot time routing: initialize a router, a multihomed host, a non router and enable IP forwarding and routing, additionally, given a scenario, troubleshoot router configuration.
- 2.7 Explain the IPv6 addressing to include IPv6 autoconfiguration, unicast, and multicast address types.
- 2.8 Configure and troubleshoot IPv6 non-routers, routers, and IPv6 6to4 routers.
- 2.9 Manage IPv6 (display critical information and modify, configure, and troubleshoot interfaces).
- 2.10 Configure IPv6 multipathing both manually and at boot time.
- 2.11 Explain the types of protocols found in the Transport layer and examine TCP flow control.

Section 3: Configure and Manage Network Applications (Application layer)

- 3.1 Explain the DNS basics (BIND, top level domains, zones of authority, server types, answer types, name resolution process, and resource records)
- 3.2 Given a scenario, configure and troubleshoot a DNS server.
- 3.3 Given a specific network, configure a DHCP server using appropriate utilities, and configure and manage DHCP clients.
- 3.4 Troubleshoot DHCP server, DHCP client, and acquire a new lease manually.
- 3.5 Configure an NTP server and an NTP client, and given a scenario, troubleshoot NTP using messages and snoop.

Section 4: Configure Solaris IP Filter

- 4.1 Configure the behavior of Solaris IP Filter using packet direction (in keywords and out keywords), and using rule processing (block keywords, pass keywords, quick keywords, and group keywords)
- 4.2 Configure and modify filtering on an IP address, network interface, protocol type, and port.
- 4.3 Configure logging in Solaris IP Filter, passed packets, blocked packets, and rule match and analyze logged information and statistics.

http://www.sun.com/training/certification/solaris/beta_objectives.html#302