Interconnecting Cisco Networking Devices Part 1 (100-101)

Exam Description: The 100-101 "Interconnecting Cisco Networking Devices Part 1" (ICND1) is a 1.5-hour exam with 50−60 questions. The 100-101 "Interconnecting Cisco Networking Devices Part 1" (ICND1) exam is associated with the Cisco Certified Entry Network Technician (CCENT®) certification and is a tangible first step in achieving an Associate-level certification. Candidates can prepare for this exam by taking the "Interconnecting Cisco Networking Devices Part 1" (ICND1) v2.0 course. This exam tests a candidate's knowledge and skills required to successfully install, operate, and troubleshoot a small branch office network. The exam includes topics on the operation of IP data networks, LAN switching technologies, IPv6, IP routing technologies, IP services (DHCP, NAT, ACLs), network device security, and basic troubleshooting. The exam is closed book and no outside reference materials are allowed.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

6% 1.0 Operation of IP Data Networks

1.1 Recognize the purpose and functions of various network devices such as routers, switches, bridges and hubs

1.2 Select the components required to meet a given network specification

1.3 Identify common applications and their impact on the network

1.4 Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models

1.5 Predict the data flow between two hosts across a network

1.6 Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN

21% 2.0 LAN Switching Technologies

2.1 Determine the technology and media access control method for Ethernet networks

2.2 Identify basic switching concepts and the operation of Cisco switches

- 2.2.a Collision domains
- 2.2.b Broadcast domains
- 2.2.c Ways to switch
  - 2.2.c (i) Store
  - 2.2.c (ii) Forward
  - 2.2.c (iii) Cut through
  - 2.2.c (iv) CAM Table

2.3 Configure and verify initial switch configuration including remote access management
- 2.3.a hostname
- 2.3.b mgmt ip address
- 2.3.c Ip default-gateway
- 2.3.d local user and password
- 2.3.e enable secret password
- 2.3.f console and VTY logins
- 2.3.g exec-timeout
- 2.3.h service password encryption
- 2.3.i copy run start

2.4 Verify network status and switch operation using basic utilities such as
- 2.4.a ping
- 2.4.b telnet
- 2.4.c SSH

2.5 Describe how VLANs create logically separate networks and the need for routing between them
- 2.5.a Explain network segmentation and basic traffic management concepts

2.6 Configure and verify VLANs

2.7 Configure and verify trunking on Cisco switches
- 2.7.a DTP (topic)
- 2.7.b Auto-negotiation

11% 3.0 IP addressing (IPv4/IPv6)

3.1 Describe the operation and necessity of using private and public IP addresses for IPv4 addressing

3.2 Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

3.3 Identify the appropriate IPv4 addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment

3.4 Describe the technological requirements for running IPv6 in conjunction with IPv4
- 3.4.a Dual stack

3.5 Describe IPv6 addresses
- 3.5.a Global unicast
- 3.5.b Multicast
- 3.5.c Link local
- 3.5.d Unique local
- 3.5.e EUI 64
- 3.5.f Auto-configuration

26% **4.0 IP Routing Technologies**

4.1 Describe basic routing concepts.
- 4.1.a Packet forwarding
- 4.1.b Router lookup process
- 4.1.c Process Switching/Fast Switching/CEF

4.2 Configure and verify utilizing the CLI to set basic Router configuration
- 4.2.a Hostname
- 4.2.b Local user & password
- 4.2.c Enable secret password
- 4.2.d Console & VTY logins
- 4.2.e exec-timeout
- 4.2.f service password encryption
- 4.2.g Interface IP Address
  - 4.2.g (i) loopback
- 4.2.h banner
- 4.2.i motd
- 4.2.j copy run start

4.3 Configure and verify operation status of an Ethernet interface

4.4 Verify router configuration and network connectivity using
- 4.4.a ping
  - 4.4.a (i) Extended ping
- 4.4.b traceroute
- 4.4.c telnet
- 4.4.d SSH
- 4.4.e Show cdp neighbors

4.5 Configure and verify routing configuration for a static or default route given specific routing requirements

4.6 Differentiate methods of routing and routing protocols
- 4.6.a Static vs. dynamic
- 4.6.b Link state vs. distance vector
- 4.6.c Next hop
- 4.6.d Ip routing table
- 4.6.e Passive interfaces (how they work)

4.7 Configure and verify OSPF (single area)
- 4.7.a Benefit of single area
- 4.7.b Configure OSPv2 in a single area
- 4.7.c Configure OSPv3 in a single area
- 4.7.d Router ID
- 4.7.e Passive interface

4.8 Configure and verify interVLAN routing (router on a stick)
- 4.8.a Sub interfaces

4.8.b Upstream routing
4.8.c Encapsulation

4.9 Configure SVI interfaces.

8% 5.0 IP Services

5.1 Configure and verify DHCP (IOS router)
- 5.1.a Configuring router interfaces to use DHCP
- 5.1.b DHCP options (Basic overview and functionality)
- 5.1.c Excluded addresses
- 5.1.d Lease time

5.2 Describe the types, features, and applications of ACLs
- 5.2.a Standard (editing and sequence numbers)
- 5.2.b Extended
- 5.2.c Named
- 5.2.d Numbered
- 5.2.e Log option

5.3 Configure and verify ACLs in a network environment
- 5.3.a Named
- 5.3.b Numbered
- 5.3.c Log option

5.4 Identify the basic operation of NAT
- 5.4.a Purpose
- 5.4.b Pool
- 5.4.c Static
- 5.4.d 1 to 1
- 5.4.e Overloading
- 5.4.f Source addressing
- 5.4.g One-way NAT

5.5 Configure and verify NAT for given network requirements

5.6 Configure and verify NTP as a client

15% 6.0 Network Device Security

6.1 Configure and verify network device security features
- 6.1.a Device password security
- 6.1.b Enable secret vs. enable
- 6.1.c Transport
  - 6.1.c (i) Disable telnet
  - 6.1.c (ii) SSH
- 6.1.d VTYs
- 6.1.e Physical security
- 6.1.f Service password
- 6.1.g Describe external authentication methods

6.2 Configure and verify switch port security
- 6.2.a Sticky mac
- 6.2.b MAC address limitation
- 6.2.c Static/dynamic
- 6.2.d Violation modes
  - 6.2.d (i) Err disable
  - 6.2.d (ii) Shutdown
  - 6.2.d (iii) Protect restrict
- 6.2.e Shutdown unused ports
- 6.2.f Err disable recovery
- 6.2.g Assign unused ports in unused VLANs
- 6.2.h Putting Native VLAN to other than VLAN 1

6.3 Configure and verify ACLs to filter network traffic

6.4 Configure and verify ACLs to limit telnet and SSH access to the router

13% 7.0 Troubleshooting

7.1 Troubleshoot and correct common problems associated with IP addressing and host configurations

7.2 Troubleshoot and resolve VLAN problems
- 7.2.a Identify that VLANs are configured
- 7.2.b Verify port membership is correct
- 7.2.c Correct IP address is configured

7.3 Troubleshoot and resolve trunking problems on Cisco switches
- 7.3.a Verify correct trunk states
- 7.3.b Verify correct encapsulation is configured
- 7.3.c Correct VLANs are allowed

7.4 Troubleshoot and resolve ACL issues
- 7.4.a Verify statistics
- 7.4.b Verify permitted networks
- 7.4.c Verify direction
  - 7.4.c (i) Interface

7.5 Troubleshoot and resolve Layer 1 problems
- 7.5.a Framing
- 7.5.b CRC
- 7.5.c Runts
- 7.5.d Giants
- 7.5.e Dropped Packets
- 7.5.f Late Collisions
- 7.5.g Input/Output errors