



Cram Guide for Exam 640-801 - Cisco Certified Network Associate Exam (CCNA 640-801)

Planning & Designing

Design a simple LAN using Cisco Technology.

1. CCNA mainly deals with routing and switching.
 - Routing takes place at layer 3.
 - Switching takes place at layer 2.
2. Cisco gears use standardized interface known as IOS.

Design an IP addressing scheme to meet design requirements.

3. In a Class A address, the first octet is the network portion. In a Class B address, the first two octets are the network portion. In a Class C address, the first three octets are the network portion.
4. In a Class A address, the first octet is the network portion. In a Class B address, the first two octets are the network portion. In a Class C address, the first three octets are the network portion.

Select an appropriate routing protocol based on user requirements.

5. Routing Information Protocol (RIP) is easy to setup but is limited by hop counts.
6. RIP 2 allows more information to be included in RIP packets and provides a simple authentication mechanism that is not supported by RIP.
7. OSPF is good for larger network where scalability is a concern. It is complicated to set up though.
8. OSPF is good for larger network where scalability is a concern. It is complicated to set up though
9. Cisco believes that IGRP is technically better than RIP, although RIP is more frequently tested in the exam.

Design a simple internetwork using Cisco technology.

10. You need to use router to connect different networks together.
11. You need to take care of IP addresses subnet configuration and routing table configuration. You may also need to deploy routing protocols.
12. EIGRP (Enhanced Interior Gateway Routing Protocol) and IGRP (Interior Gateway Routing Protocol) are Cisco proprietary routing protocols, while RIP and OSPF are open standards.

Develop an access list to meet user specifications.

13. In IP Access Lists (ACLs), masks are used with IP addresses to specify what should be permitted and denied.
14. Masks to configure IP addresses on interfaces start with 255 and have the large values on the left side. Masks for IP ACLs are the reverse (wildcard mask).

15. New ACL statements should be added to the end of the list.**Identify the procedures for installing Windows 9x/Me, Choose WAN services to meet customer requirements.**

16. A WAN is a network that covers a relatively broad geographic area that often uses transmission facilities provided by common carriers.
17. A point-to-point link provides a single pre-established WAN communications path from the customer premises to a remote network. It is usually leased from a carrier and thus is often called leased line.
18. Switched circuits allow data connections to be initiated when needed and terminated when completed. Integrated Services Digital Network (ISDN) is an example of circuit switching.
19. Packet switching is a WAN technology in which users share common carrier resources (thus cheaper to use). Examples include Transfer Mode (ATM), Frame Relay and X.25.
20. Dialup services are cost-effective solutions for connectivity across WANs and are often used when cost is a concern and usage is not frequent. Two popular examples are dial-on-demand routing (DDR) and dial backup.

Implementation & Operation

Configure routing protocols given user requirements.

21. To configure RIP, the REQUIRED steps are:
 - Enabling RIP
 - Allowing Unicast Updates for RIP
22. To configure RIP, the OPTIONAL steps are:
 - Applying Offsets to Routing Metrics
 - Adjusting Timers
 - Specifying a RIP Version
 - Enabling RIP Authentication
 - Configuring Route Summarization on an Interface
 - Verifying IP Route Summarization
 - Disabling Automatic Route Summarization
23. To configure IGRP, the REQUIRED steps are:
 - Creating the IGRP Routing Process
 - Applying Offsets to Routing Metrics
 - Allowing Unicast Updates for IGRP
 - Defining Unequal-Cost Load Balancing
 - Controlling Traffic Distribution
 - Adjusting the IGRP Metric Weights
 - Adjusting Timers
24. To configure IGRP, the OPTIONAL steps are:
 - Disabling Holddown

- Enforcing a Maximum Network Diameter
- Validating Source IP Addresses
- Enabling or Disabling Split Horizon

Running IGRP and RIP Concurrently.

25. Multi-protocol routing is common for scenarios such as mergers, multi-admin and multi-vendor environments.
26. RIP metric is based on hop count, but IGRP uses a composite metric based on bandwidth, delay, reliability, load, and maximum transmission unit (bandwidth and delay are the only parameters used by default).
27. When redistributing routing protocols, you must define a metric that is understandable to the receiving protocol through the redistribute command.

Disabling the Validation of Source IP Addresses.

28. By default the system validates the source IP addresses of incoming routing updates. To disable this function, use "no validate-update-source".

Enabling or Disabling Split Horizon.

29. Routers that use distance-vector routing protocols commonly employ the split horizon mechanism to reduce routing loops. Split horizon is a technique that blocks information about routes from being advertised by a router out of any interface from which that information originated.
30. "ip split-horizon" allows you to enable split horizon.
31. "no ip split-horizon" allows you to disable split horizon.

Configuring Interpacket Delay.

32. You may change the interpacket delay for RIP updates sent through the output-delay command in router configuration mode. You may then remove the delay with the no form of the command.

Connecting RIP to a WAN.

33. RIP is mostly for LAN due to the fact that it limits the number of router hops between any two hosts in an internet to 16. Moreover, it is slow to converge - it takes a relatively long time for network changes to become known to all routers.
34. To connect networks across WAN, you need Border Gateway Protocol (BGP). BGP performs interdomain routing between multiple autonomous systems and exchanges routing and reachability information with other BGP systems.

Configure IP addresses, subnet masks, and gateway addresses on routers and hosts.

35. An IP address is the unique number ID assigned to one host or interface in a network. It is 32 bit based.
36. A subnet is a portion of a network sharing a particular subnet address.
37. A subnet mask is a 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.
38. Every IP address is made up of 32 binary bits which can be divisible into a network portion and host portion. The 32 binary bits are broken into four octets, with 1 octet = 8 bits.
39. An interface refers to a network connection.
40. Gateway address is the router's address. A client must have a default gateway setting in order to communicate with the outside network.

Configure a router for additional administrative functionality.

41. Some layer 3 capable Cisco gears provide comprehensive Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) administrative functionality to help customers automate and streamline IP networking services, such as client configuration and provisioning.
42. DNS is for name resolution while DHCP is for dynamic IP address configuration.

Configure a switch with VLANs and inter-switch communication.

43. Virtual LAN (VLANs) refers to a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on different LAN segments. As VLANs are based on

- logical connections, they are extremely flexible in terms of configuration and application.
44. VLAN Trunking Protocol (VTP) works at Layer 2 to manage the addition, deletion, and renaming of VLANs on a network-wide basis.
 45. Generic VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

Implement a LAN.

46. Ethernet refers to LAN products covered by the IEEE 802.3 standard. Available data rates include 10 Mbps—10Base-T Ethernet, 100 Mbps—Fast Ethernet.
47. 1000 Mbps and 10,000Mbps—Gigabit Ethernet.
48. An Unshielded Twisted Pair (UTP) cable has four pairs of wires twisted inside it to eliminate electrical interference.
49. RJ-45 connectors have eight connector pins.
50. A straight-through cable connects the source and destination computers through a hub or a switch.
51. A crossover cable has the standard RJ-45 cable between source and destination cross-connected.
52. A rollover cable is a Cisco proprietary cable that connects to a router or switch console port.
53. Collision is used by Ethernet to control access and allocate shared bandwidth among stations that try to transmit at the same time on a shared medium. Ethernet uses Carrier Sense Multiple Access/Collision Detect (CSMA/CD) as its collision detection method.

Customize a switch configuration to meet specified network requirements.

54. Depending on the switch models you deploy, different commands may be used.
55. On Catalyst switches, IOS commands are different from CatOS commands.

Manage system image and device configuration files.

56. To display the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting, use the show boot command.
57. To copy the running configuration file to another destination, use the copy running-config command.
58. To copy a file from Flash memory to another destination, use the copy flash command.
59. To verify the checksum of Flash memory, use the verify flash command.
60. To enable autoloading of configuration files from a network server, use the service config command.

Perform an initial configuration on a router.

61. Different models of Cisco routers require different initial configuration tasks.
62. You may build most straightforward router configurations and create a configuration file using the router's setup facility.
63. You may use Cisco's Configuration Builder in Windows to create configuration files for multiple routers without knowing the router command-line language or syntax.
64. To return a Cisco router to its original factory defaults, you either use the config-register 0x2102 command or the config-register 0x2142 command.

Perform an initial configuration on a switch.

65. Different models of Cisco switches require different initial configuration tasks.
66. You can configure the switch from a direct console connection to the console port or remotely through its management port (if available).
67. If you are using a direct console connection, you should configure your terminal emulation program for 9600 baud, 8 data bits, no parity, and 1 stop bit.
68. If you are configuring the management port, you must assign an IP address to any Fast Ethernet or Gigabit Ethernet port on the switch.

69. You may access the Command Line Interface (CLI) on an unconfigured switch by placing the switch in Express Setup mode and then by connecting a switch Ethernet port to the Ethernet port of your workstation. Note that Express Setup is only supported on switches running IOS Release 12.1(14)EA1 or later.

Implement access lists.

70. IP Standard 1-99
71. IP Extended 100-199
72. IPX Standard 800-899
73. IPX Extended 900-999
74. IPX SAP Filters 1000-1099
75. Always remember, access list processing is sequential.

Implement simple WAN protocols.

76. WAN protocols supported by most Cisco gears include Asynchronous Transfer Mode (ATM), Frame Relay, High-Level Data Link Control (HDLC), Integrated Services Digital Networks (ISDN), Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Switched Multimegabit Data Service (SMDS), X.25 and its derivatives.

Troubleshooting

Utilize the OSI model as a guide for systematic network troubleshooting

77. A physical layer problem means a hardware and/or cable connectivity problem.
78. A layer 2 problem usually means a problem associated with LAN switching.
79. A layer 3 problem usually means a problem associated with IP addressing or routing.
80. A layer 4 problem has to deal with the application.

Perform LAN and VLAN troubleshooting.

81. For LAN, make sure that the hub or switch is properly powered and that the LAN cables are properly connected.
82. If a loop exists within an Ethernet network, a single packet that loops endlessly can cause broadcast storm and render the network useless.
83. For VLAN, always make sure that the configuration revision of all switches inserted into the VTP domain is lower than the configuration revision of the switches already in the VTP domain.

Troubleshoot routing protocols.

84. Check the routing metrics. Different routing protocols use different routing metrics.
85. The traceroute command is useful for checking routes taken by traveling packets.
86. RIP converges slowly - routing loops can occur by disagreement over the next routing hop to be taken.

Troubleshoot IP addressing and host configuration.

87. Errors mostly occur when the subnet masks are not properly configured.
88. An IP address must be unique in the network.
89. If DHCP is used, is the DHCP server distributing addresses?
90. How about the routing table entries and default gateway settings on the clients?

Troubleshoot a device as part of a working network.

91. The ping (Packet InterNet Groper) command is used for troubleshooting the accessibility of devices. The extended ping is used to perform a more advanced check of host reachability and network connectivity.
92. The traceroute command is used to discover the paths packets take to a remote destination, as well as where routing breaks down. An extended traceroute command is used to see what path packets are taking to get to a destination and to check routing.

Troubleshoot an access list.

93. Did you set up the masks for IP ACL correctly?
94. Note that traffic is compared to ACL entries based on the order that the entries occur in the router. The router continues to look until it has a match and then stops. Are your entries properly placed?

Perform simple WAN troubleshooting.

95. Different WAN protocols require different troubleshooting methods. Common troubleshooting techniques: Is the WAN line up? Is it in loopback mode (if so, turn off the loopback mode)? Any alarms or error events? Did you deploy compression or encryption (watch out for hardware and software compatibility)?

Technology

Describe network communications using layered models.

96. Cisco has defined a hierarchical model known as the hierarchical internetworking model for simplifying the task of building a reliable and scalable hierarchical internetwork.
97. The 3 layers model focuses on the three functional areas, namely the Core layer, the Distribution layer and the Access layer.

Describe the Spanning Tree process.

98. Spanning-Tree Protocol (STP) has the goal of preventing loops from being formed when switches or bridges are interconnected via multiple paths and ensuring that only one active path exists between two network devices.
99. STP implements the 802.1D IEEE algorithm by exchanging BPDU messages with other switches to detect loops and then removes the loop by shutting down selected bridge interfaces.

Compare and contrast key characteristics of LAN environments.

100. A LAN is a computer network that spans a relatively small area.
101. Most LANs are confined to a single physical location.
102. The characteristics that differentiate one LAN from another include topology, protocols and cable media.
103. LANs allows data transmission at very fast rates, but the distances and the number of computers are limited.

Evaluate the characteristics of routing protocols.

104. Interior Routing Protocols (IGPs) operate within autonomous systems. Examples are RIP, IGRP, Enhanced IGRP, OSPF and Integrated IS-IS.
105. Exterior Routing Protocols (EGPs) provide routing between autonomous systems. The two most popular EGPs in the TCP/IP community are BGP and EGP.
106. Translation between environments with different routing protocols requires that routes generated by one protocol be redistributed into the second routing protocol environment.

Evaluate TCP/IP communication process and its associated protocols.

107. TCP is a connection-oriented transport protocol. It sends data as an unstructured stream of bytes. With sequence numbers and acknowledgment messages, TCP can provide a sending node with delivery information about packets transmitted to the destination.
108. In the case of packet lost in transit, TCP can perform re-transmission until either a timeout condition is reached or until successful delivery has been achieved. TCP can also recognize and discard duplicate messages.
109. Cisco TCP/IP implementation supports ARP, RARP, ICMP, Proxy ARP, Echo, Discard, and Probe.

Describe the components of network devices.

110. Different network devices have different components. Hardware components include memory, processor and circuit board, while software components include firmware and IOS.

Evaluate rules for packet control.

111. Depending on purposes, packet control can involve different rules.
112. We may control packets for bandwidth usage control, for security, or for other purposes.
113. Packet control often takes place at the gateway and can involve significant processing overhead.

Evaluate key characteristics of WANs

114. WAN covers a broad geographic area that often uses

transmission facilities provided by common carriers.

115. WAN technologies generally function at the lower three OSI layers.
116. Many WANs deploy virtual circuits - logical circuits created within shared networks between two network devices. The two major types of virtual circuits are switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).
117. WANs require numerous types of device that are specific to WAN environments, such as WAN switches, access servers, modems, CSU/DSUs, and ISDN terminal adapters.