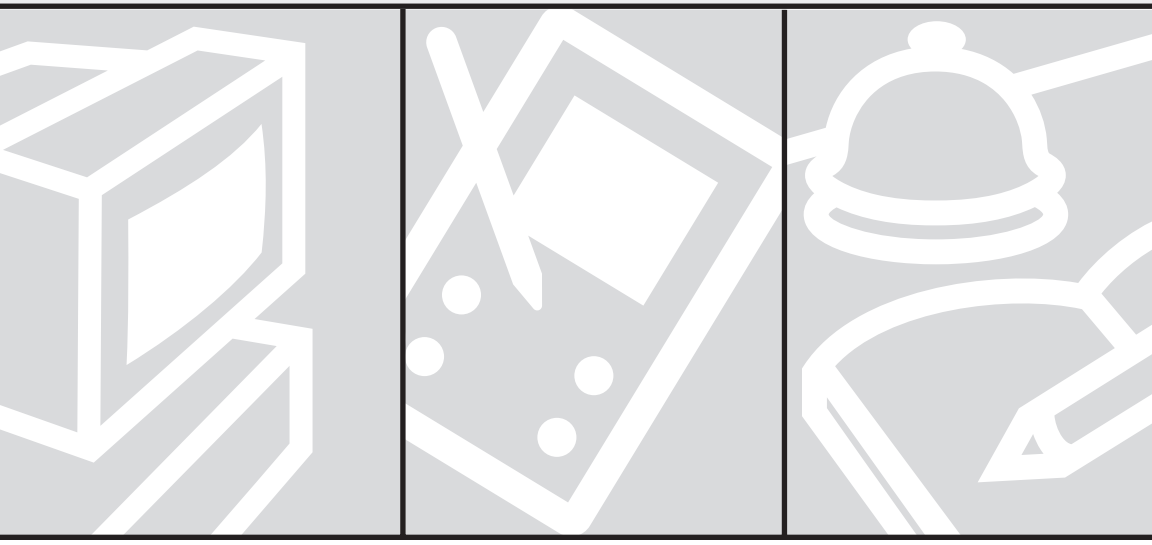

Section 1
General Networking Theory

This chapter ensures you are prepared for questions in the Cisco Certified Internetwork Expert (CCIE) written exam that deal with general networking theories. General networking theories include Open System Interconnection (OSI) models, routing concepts, networking standards, and protocol mechanics.

As you might expect, many of the concepts reviewed in this chapter receive additional and more specific coverage elsewhere in this text. It is critical that you review the topics at this level as well, however. The information contained here is not repeated later at all.

The CCIE—Routing/Switching candidate should have several years of hands-on experience with Cisco gear. Therefore, this section also ensures you are well-versed in Cisco device operations. This section focuses on general **show** and **debug** commands and their usage, as well as physical structures within almost all Cisco equipment. It also reviews basic device operational characteristics including device access, password recovery, Simple Network Management Protocol (SNMP), and Switched Port Analyzer (SPAN).

Question 1

Name the seven layers of the OSI model in order from top to bottom.

Question 2

Name the four layers of the Department of Defense (DoD) TCP/IP model in order from top to bottom.

Question 3

The Process/Application layer of the TCP/IP reference model encompasses the functionality of which OSI reference model layers?

Question 1 Answer

The seven layers of the OSI model from top to bottom are:

Application

Presentation

Session

Transport

Network

Data link

Physical

Question 2 Answer

The four layers from top to bottom are:

Process/Application

Host to Host

Internet

Network Access

Question 3 Answer

The Process/Application layer incorporates the functionality of the application, presentation, and session layers.

Question 4

The Host to Host layer of the TCP/IP reference model incorporates the functionality of which OSI layer?

Question 5

The network layer of the OSI reference model incorporates the functionality of which TCP/IP reference model layer?

Question 6

The Network Access layer of the TCP/IP reference model incorporates the functionality of which OSI reference model layers?

Question 4 Answer

The Host to Host layer incorporates the functionality of the transport layer.

Question 5 Answer

The Internet layer of the TCP/IP model is the equivalent of the OSI model's network layer.

Question 6 Answer

The Network Access layer is associated with the physical and data link layers of the OSI model.

Question 7

The IEEE 802.2 specification defines which sublayer of the data link layer of the OSI reference model?

Question 8

Which layer of the OSI reference model is responsible for path selection through an internetwork?

Question 9

Name four distance vector routing protocols.

Question 7 Answer

The IEEE 802.2 specification defines the logical link control (LLC) sublayer of the data link layer. IEEE 802.2 defines a number of fields in data link layer frames that enable multiple higher-layer protocols to share a single physical data link.

Question 8 Answer

The Network layer is responsible for path selection through the internetwork.

Question 9 Answer

Distance vector routing protocols include:

RIP version 1

RIP version 2

IGRP

EIGRP (Advanced Distance Vector)

BGP (Advanced Distance Vector)

Question 10

Name two link state routing protocols.

Question 11

Name three attributes typical of classic distance vector routing protocols.

Question 12

Name at least three attributes of link state routing protocols.

Question 10 Answer

Link state routing protocols include:

OSPF

IS-IS

Question 11 Answer

Classic distance vector routing protocols exhibit these attributes:

Defined finite hop count

Convergence tends to be slower

Periodic broadcast of routing tables

Many loop prevention mechanisms

Communication of routing table information with directly connected neighbors

Question 12 Answer

The following are all attributes of link state routing protocols:

More scalable because of no hop count limitations

Convergence tends to be quicker

Triggered multicast of routing information changes

Fewer loop prevention mechanisms required typically

Flooding of link information to all devices in the routing domain

Local databases used to derive best route information using the shortest path first algorithm

Question 13

What is the default administrative distance of a directly connected route?

Question 14

What is the default administrative distance of a static route that points to a next hop router?

Question 15

What is the default administrative distance of an Enhanced Interior Gateway Routing Protocol (EIGRP) summary route?

Question 13 Answer

0

Question 14 Answer

1

Question 15 Answer

5

Question 16

What is the default administrative distance of External Border Gateway Protocol (BGP)?

Question 17

What is the default administrative distance of Internal EIGRP?

Question 18

What is the default administrative distance of Interior Gateway Routing Protocol (IGRP)?

Question 16 Answer

20

Question 17 Answer

90

Question 18 Answer

100

Question 19

What is the default administrative distance of Open Shortest Path First (OSPF)?

Question 20

What is the default administrative distance of Intermediate System-to-Intermediate System (IS-IS)?

Question 21

What is the default administrative distance of Routing Information Protocol (RIP)?

Question 19 Answer

110

Question 20 Answer

115

Question 21 Answer

120

Question 22

What is the default administrative distance of External EIGRP?

Question 23

What is the default administrative distance of Internal BGP?

Question 24

What is a floating static route?

Question 22 Answer

170

Question 23 Answer

200

Question 24 Answer

A floating static route is a static route with an administrative distance assigned that is higher than the administrative distance of the dynamic routing protocol in use. This allows the static route to act as a backup route in the event of a link failure.

Question 25

Define split horizon.

Question 26

What is poison reverse?

Question 27

Name at least three advantages of route summarization.

Question 25 Answer

Split horizon refers to a routing protocol's not sending updates out an interface where the updates were originally received.

Question 26 Answer

Poison reverse is an exception to the split horizon rule. Poisoned routes are sent out an interface from where the update was originally received.

Question 27 Answer

Route summarization provides the following advantages:

Smaller routing tables (less memory required)

Less overhead for routers performing lookups

Causes fewer routing updates by hiding details of subnet status

Promotes the use of variable-length subnet mask (VLSM)

Enables classless interdomain routing (CIDR)

Question 28

If a router contains a route entry for the specific host address, a route entry for the subnet, and a summarized route entry for the major classful network, which route entry does the router use?

Question 29

What is tunneling?

Question 30

100BASE-TX requires what type of physical media?

Question 28 Answer

The router relies upon the longest match (of subnet mask) principle when evaluating routes. In this case—the host entry has the longest subnet mask and, therefore, is the route that is selected.

Question 29 Answer

Tunneling refers to further encapsulating header, data, and trailer information to carry this private information securely across a public network. The original packet with its encapsulation information appears as data in the tunnel.

Question 30 Answer

100BASE-TX requires Cat 5 unshielded twisted-pair (UTP) or Type 1 shielded twisted-pair (STP) wire.

Question 31

Is the TCP "handshake" process one way, two way, or three way?

Question 32

Which of the TCP hosts (sender or receiver) sets the SYN bit in the communication?

Question 33

Under the concept of "sliding windows" in TCP/IP, does the sender or receiver specify the window size?

Question 31 Answer

The TCP handshake process is three way. The TCP handshake is made up of three TCP segments exchanged between two devices; the initial SYN, a SYN/ACK, and an ACK.

Question 32 Answer

The sender sets the SYN bit to indicate that a connection request is being made. The receiver sets the SYN bit in its SYN/ACK response to the SYN packet.

Question 33 Answer

With TCP/IP sliding windows, the receiver specifies the current window size in every packet. The window is the number of data bytes that the sender is allowed to send before waiting for an acknowledgment.

Question 34

How does a receiver indicate to the sender not to send any data (using sliding windows)?

Question 35

If a TCP/IP sender transmits bytes 6 through 11 and these bytes are received successfully by the receiver, what acknowledgment number should be sent back to the sender?

Question 36

What does MTU refer to?

Question 34 Answer

The receiver indicates a window size of 0.

Question 35 Answer

The receiver should send an ACK = 12 to indicate that the next byte expected is 12.

Question 36 Answer

MTU refers to maximum transmission unit. MTU is the largest size packet or frame that can be sent in a network.

Question 37

Name two possible issues that can be caused by fragmentation.

Question 38

Which bit in the FLAGS field of the TCP/IP header indicates that the connection should be terminated?

Question 39

What is Q-in-Q tunneling and when might it be used?

Question 37 Answer

Possible issues include:

Overhead due to reassembly

Lost fragments

Firewalls permitting or denying non-initial fragments

Question 38 Answer

The FIN bit resides in the FLAGS field and is used for termination.

Question 39 Answer

Q-in-Q tunneling refers to tunneling an 802.1q packet inside another 802.1q packet to distinguish different customer's virtual LANs (VLANs). Providers might use this mechanism if they are providing Metro Ethernet service to multiple customers for high speed metropolitan-area network (MAN) connectivity.

Question 40

What is the default hop count limit used in RIP v2 networks?

Question 41

The use of keepalives on a serial interface can cause interface failures. What common show command checks to see if keepalives are set on the interface?

Question 42

What field in the show interface command output for a Fast Ethernet interface might indicate that cable runs are too long?

Question 40 Answer

The default is 15.

Question 41 Answer

The **show interface** command output features a Keepalive field used to indicate whether keepalives are set or not. If keepalives are set too low and considerable congestion exists on an opposing interface, keepalives might not be returned in time—causing interface failures.

Question 42 Answer

The Late Collisions field indicates the number of collisions that occur after transmitting the preamble; large numbers of late collisions often indicate that cable runs are too long or a duplex mismatch exists.

Question 43

Considering the show interface command—what field allows the analysis of the error rates reported to determine the true volume of damaged frames sent or received?

Question 44

What does the Overrun field indicate in a show interface command result?

Question 45

What command permits the determination of the type of interface processors installed in a Cisco 7500 series router?

Question 43 Answer

Use the Last Cleared field to see how long the counters have been tracking error conditions. The **clear counters** command allows you to reset the counters in these **show** commands.

Question 44 Answer

The Overrun field indicates the number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.

Question 45 Answer

The **show diag** command permits the evaluation of interface types in the 7500 series.

Question 46

You can identify the feature set loaded on a particular router with the show version command. What does a jk8s in the image name typically indicate?

Question 47

A Cisco 7200 series router possesses an image name that contains the following portion:

c7200-ajs40-mz

What does the mz portion of this image name indicate?

Question 48

Cisco releases software in trains. This allows them to introduce new features in some software, while just fixing bugs in other releases. What is the purpose of an E train?

Question 46 Answer

This typically indicates the Enterprise Plus IPSec 56 feature set is in use. Common naming conventions for feature sets include:

IP Plus—is

IP—i

Enterprise Plus IPSec 56—jk8s

Enterprise Plus—js

Enterprise—j

Question 47 Answer

This portion of the name indicates the run-time memory in use and compression format. Here are common examples:

F—Image runs in Flash

m—Image runs in RAM

R—Image runs in ROM

L—Image is located at run time

z—Image is Zip compressed

x—Image is Mzip compressed

w—Image is STAC compressed

Question 48 Answer

The E train targets enterprise core and SP edge devices. This train supports advanced quality of service (QoS), voice, security, and firewall capabilities. This train fixes defects found in previous versions.

Other trains include:

mainline—Consolidates releases and fixes defects. Inherits features from the parent T train and does not add additional features.

T—Introduces new features and fixes defects.

S—Consolidates 12.1E, 12.2 mainline, and 12.0S, which supports high-end backbone routing and fixes defects.

E—Targets enterprise core and SP edge, supports advanced QoS, voice, security, and firewall, and fixes defects.

Question 49

How many images are required for the supervisor engine and the MSFC daughter card in a Cat 6500 series router running native IOS?

Question 50

Debug messages are sent to the console port by default. What command allows these messages to appear on a Telnet session?

Question 51

What is the most efficient method for logging on a Cisco device?

Question 49 Answer

One image is required in this case because of the use of native IOS. CatOS actually uses two images. The image naming convention used in the case of native IOS is:

c6sup{Supervisor Engine Model}{MSFCModel}.<features>.<version>.bin

Question 50 Answer

The **terminal monitor** command permits **debug** output to appear on a telnet client.

Question 51 Answer

Logging to an internal buffer is the most efficient method. This is configured with the **logging buffered** command.

Question 52

A show flash command depicts many files that possess a deleted flag. How can these files be removed from Flash memory?

Question 53

What are the three options for file transfers to and from your Cisco device from rommon mode?

Question 54

When the Enter key is pressed following the command copy tftp flash, what is the prompt that appears?

Question 52 Answer

The **squeeze** command removes deleted files from Flash memory.

Question 53 Answer

Xmodem , Ymodem, and TFTP are options from rommon mode on most Cisco devices.

Question 54 Answer

Address or name of remote host []?

Question 55

You are working on a Cisco device that features access to two different PCMCIA Flash cards. How can you move from one to another in the operating system?

Question 56

What is the default password set on a Cat 5000 for the first 30 seconds following boot?

Question 57

Describe the key steps for recovering the password on most Cisco routers?

Question 55 Answer

You use the **cd** command to move from card to card. For example, **cd slot0** moves you to the card in slot 0.

Question 56 Answer

The default password for 30 seconds following boot is none—simply press the Enter key at the password prompt.

Question 57 Answer

The most common password recovery procedures involve the following steps:

Access the console port and use the Break sequence during reboot.

Change the configuration register and have the router ignore the startup configuration on the subsequent boot.

Log in to the device and enter privileged mode.

Copy the startup configuration into RAM.

Reset the configuration register.

Set the new password.

Copy the configuration to startup.

Question 58

What do the bit numbers 0–3 control in the configuration register of a Cisco router?

Question 59

What does bit number 6 control in the configuration register?

Question 60

If the configuration register is set to 0x2101, where is the Cisco IOS image booted from?

Question 58 Answer

Bits 0–3 control the boot characteristics. These bits are often referred to as the boot field.

Question 59 Answer

Bit 6 causes the system to ignore the configuration in nonvolatile random-access memory (NVRAM).

Question 60 Answer

If the boot field is set to 0x1 as in the example here, the router boots the ROM image.

Question 61

What command disables SNMP agent functionality on a Cisco device?

Question 62

You are interested in permitting a CiscoWorks server to obtain performance and configuration information from a Cisco router in your network. At a minimum, what command must be in place on the Cisco device?

Question 63

How does RSPAN carried mirrored traffic to the destination port?

Question 61 Answer

The command **no snmp-server** disables SNMP functionality.

Question 62 Answer

At a minimum, the device must have a read-only SNMP community string set. This is accomplished on most devices using the following command:

```
snmp-server community [string] ro
```

Question 63 Answer

RSPAN uses a special RSPAN VLAN to transport the mirrored frames to the destination port.

Question 64

What is the default spanning-tree configuration of a Switched Port Analyzer (SPAN) destination port?

Question 65

You are configuring a Catalyst 3550 switch. You have made several VLAN configurations including the creation of several VLANs and the renaming of several others. Where (specifically) are these VLAN configurations stored on the switch?

Question 64 Answer

Spanning tree is disabled for SPAN destinations. This is one reason why it is very important to reverse the configuration of SPAN once you are done analyzing traffic. Plugging a switch into a SPAN destination port can introduce switching loops.

Question 65 Answer

Configurations for VLAN IDs 1 to 1005 are written to the file vlan.dat (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The vlan.dat file is stored in Flash memory.