100-105.exam

Number: 100-105
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Cisco

100-105

NetCert: Interconnecting Cisco Networking Devices Part 1 (ICND1) v3.0

Version 1.0

Exam A

QUESTION 1
You are considering a candidate for a job as a Cisco network technician. As part of the assessment process, you ask the candidate to write down the commands required to configure a serial interface, in the proper order with the correct command prompts. The candidate submits the set of commands shown below (line numbers are for reference only):

1 Router# configure terminal
2 Router(config)# interface S0
3 Router(config)# ip address 192.168.5.5
4 Router(config-if)# enable interface
5 Router(config-if)# description T1 to Raleigh

What part(s) of this submission are incorrect? (Choose all that apply.)

A. The prompt is incorrect on line 1
B. The IP address is missing a subnet mask
C. The prompt is incorrect on line 5
D. The prompt is incorrect on line 3
E. The command on line 4 is incorrect
F. The prompt is incorrect on line 4
G. The description command must be executed before the interface is enabled

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The IP address is missing a subnet mask, the prompt is incorrect on line 3, and the command enabling the interface (line 4) is incorrect.

The correct prompts and commands are as follows:

Router# configure terminal
Router(config)#interface S0
Router(config-if)# ip address 192.168.5.5 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# description T1 to Raleigh

The prompt for line 3 would be Router(config-if)# because the interface S0 command was issued immediately prior to the ip address 192.168.5.5 command. The prompt will remain Router(config-if)# for lines 3, 4, and 5 as each command that applies to the S0 interface is executed, including the description command.

The command to enable the interface is no shutdown, not enable interface. Therefore, the command executed on line 4 was incorrect.

Objective:
Network Fundamentals

Sub-Objective:
Apply troubleshooting methodologies to resolve problems

References:

https://search.cisco.com/search?query=Cisco%20IOS%20IP%20Routing%20BFD%20Configuration%

20Guide&locale=enUS&tab=Cisco

QUESTION 2
Which of the following is NOT an advantage of static routes over dynamic routing protocols?

A. Routing protocol overhead is not generated by the router.
B. Bandwidth is not consumed by route advertisements between network devices.
C. Static routes are easier to configure and troubleshoot than dynamic routing protocols.
D. Static route configuration is more fault tolerant than dynamic routing protocols.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Static route configuration is NOT more fault tolerant than dynamic routing protocols. The following lists the true advantages of static routes over dynamic routing protocols:

- Routing protocol overhead is not generated by the router.
- Bandwidth is not consumed by route advertisements between network devices.
- Static routes are easier to configure and troubleshoot than dynamic routing protocols.
- Router resources are more efficiently used.
- Network security is increased by using static routes.

The following are disadvantages of static routes:

- Static routes are not recommended for large networks because static routes are manually configured on the router. Therefore, maintaining routes in a timely manner is nearly impossible.
- Static route configuration is not fault tolerant without configuring multiple static routes to each network with varying administrative distances.

All other options are incorrect because these are the advantages of static routes over dynamic routing protocols.

Objective:
Routing Fundamentals

Sub-Objective:
Compare and contrast static routing and dynamic routing

References:

http://docwiki.cisco.com/wiki/Routing_Basics

QUESTION 3
What configuration is needed to span a user defined Virtual LAN (VLAN) between two or more switches?

A. A VTP domain must be configured.
B. VTP pruning should be enabled.
C. The VTP mode of operation should be server.
D. A trunk connection should be set up between the switches.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To span a user defined VLAN between two or more switches, a trunk connection must be established. Trunk connections can carry frames for multiple VLANs. If the link between switches is not trunked, by default only VLAN 1 information will be switched across the link.

A VLAN trunking protocol (VTP) domain is not necessary to span VLANs across multiple switches. VTP is used to have consistent VLAN configuration throughout the domain.

VTP pruning is used to detect whether a trunk connection is carrying unnecessary traffic for VLANs that do not exist on downstream switches. By default, all trunk connections carry traffic from all VLANs in the management domain. However, a switch does not always need a local port configured for each VLAN. In such situations, it is not necessary to flood traffic from VLANs other than the ones supported by that switch. VTP pruning enables switching fabric to prevent flooding traffic on trunk ports that do not need it.

VTP server mode is not required for a server to span multiple switches. In VTP server mode of operation, VLANs can be created, modified, deleted, and other VLAN configuration parameters can be modified for the entire VTP domain. VTP messages are sent over all trunk links, and configuration changes are propagated to all switches in the VTP domain.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure,verify, and troubleshoot VLANs (normal range) spanning multiple switches

References:

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25sg/configuration/guide/conf/vlans.html

QUESTION 4
When a packet is forwarded through a network from one host to another host, which of the following fields in the Ethernet frame will change at every hop?

A. Source IP address
B. Destination MAC address
C. Source port number
D. Destination IP address

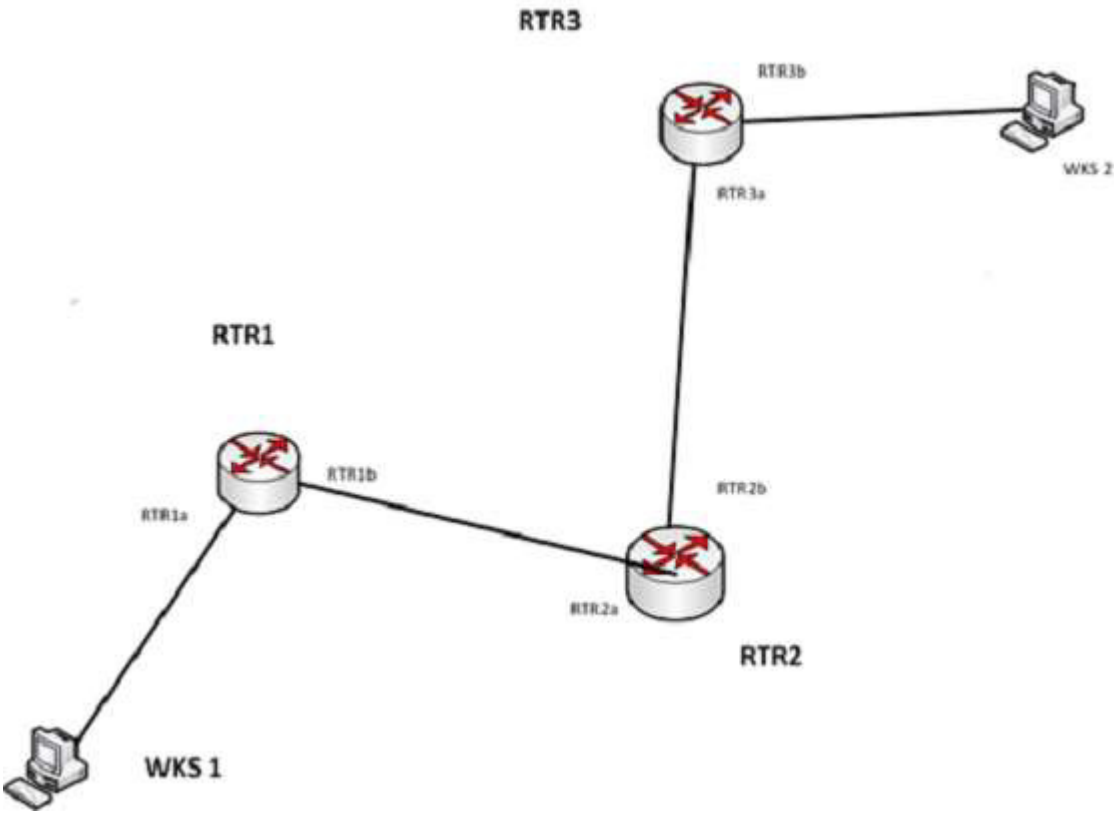
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When an Ethernet frame is forwarded through the network, both the source and destination MAC addresses will change at every hop.

The source and destination IP addresses and source and destination port numbers MUST remain the same for proper routing to occur, for the proper delivery to the destination service, and for the proper reception of responses to the sending device. By contrast, the MAC addresses used at each hop must be those of the physical interfaces involved in the Layer 2 forwarding at each hop.

As a simple illustration of this process, IP addresses and MAC addresses are assigned to two computers and three routers shown in the diagram. The network is arranged as shown below:



The IP addresses and the MAC addresses of each device are shown below:

DEVICE IP ADDRESS MAC ADDRESS
WKS1 192.168.5.5 a-a-a-a-a-a
RTR1a 192.168.5.6 b-b-b-b-b-b
RTR1b 172.16.5.5 c-c-c-c-c-c
RTR2a 172.16.5.6 d-d-d-d-d-d
RTR2b 10.6.9.5 e-e-e-e-e-e
RTR3a 10.6.9.6 f-f-f-f-f-f
RTR3b 27.3.5.9 g-g-g-g-g-g
WKS2 27.3.5.10 h-h-h-h-h-h

There will be four handoffs to get this packet from WKS1 to WKS2. The following table shows the destination IP addresses and destination MAC addresses used at each handoff.

Handoff Packet (IP) destination address Frame (MAC) Destination Address
WKS1 to RTR1a 27.3.5.10 b-b-b-b-b-b
RTR1b to RTR2a 27.3.5.10 d-d-d-d-d-d
RTR2b toRTR3a 27.3.5.10 f-f-f-f-f-f
RTR3b to WKS2 27.3.5.10 h-h-h-h-h-h

As you can see, the destination IP address in the packet does not change, but the MAC address in the frame changes at each handoff.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Interpret Ethernet frame format

References:

https://serverfault.com/questions/438141/mac-address-changes-for-every-new-network

QUESTION 5
You are creating a configuration to use on a switch. The configuration must enable you to remotely manage the switch. Which of the following command sets is correct? (Assume the commands are executed at the correct prompt.)

A. interface vlan 1ip address 192.168.20.244 255.255.255.240no shutdownexitip default-gateway 192.168.20.241line vty 0 15password ciscologinexit
B. interface fastethernet 0/1ip address 192.168.20.244 255.255.255.240no shutdownexitip default-gateway 192.168.20.241line vty 0 15password ciscologinexit
C. interface vlan 1ip address 192.168.20.244 255.255.255.240no shutdownexitip route 192.168.20.241line vty 0 15loginexit
D. interface vlan 1ip address 192.168.20.244255.255.255.240no shutdownexitip default-gateway 192.168.20.241line con 0 15password ciscologinexit
E. interface vlan 1ip address 192.168.20.244 255.255.255.240no shutdownexitip default-gateway 192.168.20.27line vty 0 15password ciscologinexit
F. interface vlan 1ip address 192.168.20.244 255.255.255.240shutdownexitip default-gateway 192.168.20.241line vty 0 15password ciscologinexit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following command set is correct:

interface vlan 1
ip address192.168.20.244 255.255.255.240
no shutdown
exit
ip default-gateway 192.168.20.241
line vty 0 15
password cisco
login
exit

It sets an IP address for VLAN 1, which is the management VLAN. Next, it sets a default gateway that is in the same network with theIP address. It correctly enables the interface, sets a required password on the VTY lines, and sets the switch to prompt for the password.

Switches do not need IP addresses unless you want to remotely manage the devices. When an IP address is assigned toa switch for this purpose, it is not applied to a physical interface. It is applied to the VLAN 1 interface, which is the management VLAN by default.

The following command set is incorrect because it applies the IP address to the fastethernet 0/1 interface, rather than the management VLAN. When you set an IP address for the switch, you do so on the management VLAN, not one of the physical interfaces.

interface fastethernet 0/1
ip address 192.168.20.244 255.255.255.240
no shutdown
exit

```
ip default-gateway192.168.20.241
line vty 0 15
password cisco
login
exit
```

The following command set is incorrect because it does not set a password on the VTY lines, which is required to connect with Telnet unless you include the no login command.

```
interface vlan 1
ipaddress 192.168.20.244 255.255.255.240
no shutdown
exit
ip default-gateway 192.168.20.241
line con 0 15
login
exit
```

The following command set is incorrect because it sets the password in the console line rather than the VTY lines.

```
interface vlan 1
ip address 192.168.20.244 255.255.255.240
no shutdown
exit
ip default-gateway 192.168.20.241
line con 0 15
password cisco
login
exit
```

The following command set is incorrect because the address for VLAN1 and the gateway are not in the same subnet. With a 28-bitmask the interval is 16, which means the network that the gateway is in is the 192.168.20.16/28 network and VLAN 1 is in the 192.1683.20.240/28 network.

```
interface vlan 1
ip address 192.168.20.244 255.255.255.240
no shutdown
exit
ip default-gateway 192.168.20.27
line vty 0 15
password cisco
login
exit
```

The following command set is incorrect because the VLAN 1 interface has been disabled with the shutdown command.

```
interface vlan 1
ip address 192.168.20.244 255.255.255.240
shutdown
exit
ip default-gateway 192.168.20.241
line vty 0 15
password cisco
login
exit
```

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure and verify device management

References:

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10594-8.html

QUESTION 6
Which keywords can be substituted for access list wildcards while configuring access lists? (Choose two.)

A. all
B. any
C. host
D. range
E. subnet

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The keywords any and host can be substituted for access list wildcards. These keywords make the access list configuration easy.

The any keyword is used for a wildcard referring to all devices. The equivalent wildcard is 255.255.255.255. For example:

Router(config)# access-list 10 deny any

or

Router(config)# access-list 15 deny 0.0.0.0 255.255.255.255

Standard access lists 10 and 15 deny packets from all source IP addresses and produce the same result.

If you have to configure an access list with only one source or destination IP address, you can use the host keyword. The host keyword is equivalent to the 0.0.0.0 wildcard. For example, if you must permit IP address 192.168.144.25, you can configure the following:

Router(config)# access-list 20 permit 192.168.144.25 0.0.0.0

or

Router(config)# access-list 20 permit host 192.168.144.25

The keywords all and subnet are invalid keywords. The keyword range cannot be used as a substitute for wild cards but it can be with access lists to specify a range of port numbers such as:

access-list 101 permit tcp any any range 1024 65535

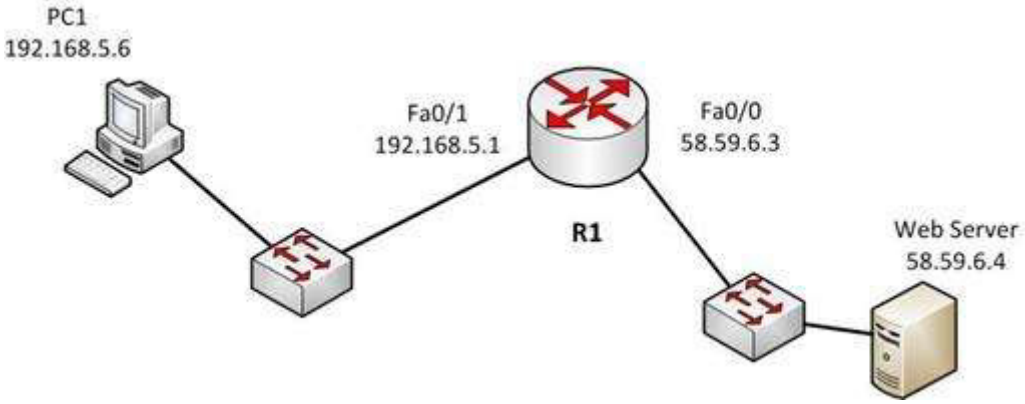
Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces

References:

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

QUESTION 7
Examine the diagram below:



You attempt to make a Telnet connection from PC1 to the switch connected to the Web server, but the connection fails. After making a console connection to the switch connected to the Web server and executing the show run command, you see the following information:

<output omitted>

interface vlan 1
ip address 58.59.6.2 255.0.0.0
!
ip default gateway 192.168.5.1
!
line vty 04
password ajax
login

Which value is NOT correct?

A. the default gateway
B. the VLAN number
C. the password
D. the login command

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The switch is connected to the F0/0/ interface on the router R1. The address of Fa0/0 should be the default gateway for the switch. This means it should be 58.59.6.4 rather than 192.168.5.1.

The VLAN number is correct. The IP address of a switch is set on the VLAN 1 interface of the switch.

The password can be anything you desire, so that is correct.

The login command is correct. This commandinstructs the switch to prompt for a password. Since there is a password configured, this will not prevent a connection to the switch.

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure and verify device management

References:

QUESTION 8
Which Cisco Internetwork Operating System (IOS) command will you use to view the details of each interface on a router?

A. show controllers
B. show interfaces ethernet
C. show ip interface brief
D. show interfaces loopback

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show ip interface brief command is used to view the details of each interface on a router. The output of the command displays the interfaces, the IP addresses configured on each interface, the method, the status, and the protocol.

The following is a sample output of this command:

Interface IP-Address OK? Method Status Protocol
Ethernet0 10.105.00.5 YES NVRAM up up
Ethernet1 unassigned YES unset administratively down down
Loopback0 10.105.200.5 YES NVRAM up up
Serial0 10.105.100.5 YES NVRAM up up
Serial1 10.105.40.5 YES NVRAM up up
Serial2 10.105.100.5 YES manual up up
Serial3 unassigned YES unset administratively down down

The show controllers command is incorrect. The show controllers command is used to view hardware-related information on router and switch interfaces. It is useful for troubleshooting and diagnosing issues with interfaces. One of the many useful pieces of information yielded by command is the type of cable connected to the interface. When you are using a V.35 cable to connect two serial interfaces directly between two routers, one of the routers must be configured to provide the clocking on the line and it must be the router with the DCE end of the cable. You can determine which router has that end by executing this command, which would display output similar to the following:

R2#show controllers serial 0
HD unit 0, idb = 0xDFE73, driver structure at 0xE52FF
Buffer size 1524 HD unit 0, V.35 DCE cable, clockrate 64000

In the above example, the DCE end of the V.35 cable is connected to this router. Therefore, this is the router that must be configured with a clockrate. The output demonstrates that this requirement was already met.

The show interfaces ethernet command is incorrect because this command will display information only for Ethernet interfaces.

The show interfaces loopback command is incorrect because this command will show information regarding loopback interfaces only.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cableissues (collisions, errors, duplex, speed)

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book/ipaddr-r1.html#wp2064770368

QUESTION 9
Which of the following situations could cause a switch to enter initial configuration mode upon booting?

A. Corrupt or missing image file in flash memory
B. Corrupt or missing configuration file in NVRAM memory
C. Corrupt or missing configuration file in flash memory
D. Corrupt or missing configuration file in ROM memory

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A missing or corrupt file in the switch's Non Volatile Random Access Memory (NVRAM) can cause the switch to enter initial configuration mode upon booting. When a Cisco switch boots up and finds no configuration file in NVRAM, it goes into initial configuration mode and prompts the user to enter basic configuration information to make the switch operational. The initial configuration mode of a switch is similar to the initial configuration mode of a router, but the configuration parameters are different.

A corrupt or missing image or configuration file in flash or ROM memory would not cause a switch to enter initial configuration mode upon booting. The IOS image file is stored in flash, and if it is corrupt or missing, the switch goes in to ROMMON mode, in which a limited version of the IOS image from ROM is loaded into RAM.

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure and verify initial device configuration

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15-s/fundamentals-15-s-book.html#wp1017984

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15-s/fundamentals-15-s-book.html

QUESTION 10
Which Cisco IOS command allows you to change the setting of the configuration register?

A. boot config
B. configuration-register edit
C. config-register

D. edit configuration-register

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The config-register command is used to change the setting of the configuration register. The configuration register has the boot field setting, which specifies the order in which the router should look for bootstrap information. The router contains a 16-bit software register, which is stored in the non-volatile random access memory (NVRAM). The config-register command is used to modify the default configuration register. The most common use of changing this register is to instruct the router to ignore the stored configuration file and boot as a new router with no configuration. This process is normally used when a router has a password that is not known and must be reset. For security purposes, this procedure can only be performed from the console connection, which means it requires physical access to the router.

Normally the setting of this register is 0x2102, which tells the router to look for a configuration file. If the file exists, it will use it. If none exists, the router will boot into ROM and present the user with a menu-based setup. This would be the default behavior for a new router as well.

To view the value of the configuration register, use the show version command as displayed below. The register setting can be seen at the bottom of the output in bold.

```
Cisco IOS Software, 3600 Software (C3660-I-M), Version 12.3(4)T
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Thu 18-Sep-03 15:37 by ccai
ROM: System Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)
ROM:
C3660-1 uptime is 1 week, 3 days, 6 hours, 41 minutes
System returned to ROM by power-on
System image file is "slot0:tftpboot/c3660-i-mz.123-4.T"

Cisco 3660 (R527x) processor (revision 1.0) with 57344K/8192K bytes of memory.
Processor board ID JAB055180FF
R527x CPU at 225Mhz, Implementation 40, Rev 10.0, 2048KB L2 Cache

3660 Chassis type: ENTERPRISE
2 FastEthernet interfaces
4 Serial interfaces
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of NVRAM.
16384K bytes of processor board System flash (Read/Write)

Flash card inserted. Reading filesystem...done.
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)

Configuration register is 0x2102
```

To change this setting would require issuing these commands, followed by a restart:

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config
Router(config)#config-register 0x2142

By setting register to 0x2142, the router will ignore a configuration file at reboot if it exists. The router will then enter setup mode and prompt for you to enter initial system configuration information, as would happen with a new router. This enables the user to bypass an unknown password, since the password is contained in the file.

The boot config command is incorrect because this command is used to set the device where the configuration file is located (flash, slot, etc.) and file name for the configuration file, which helps the router to configure itself during startup.

The configuration-registeredit command and the edit configuration-register commands are incorrect because they are not valid Cisco IOS commands.

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

References:

https://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html#config-reg-meaning

QUESTION 11
Which Ethernet LAN contention or access method listens for a signal on the channel before transmitting data, and stops transmitting if a collision is detected?

A. CSMA/CA
B. CSMA/CD
C. CSMA/CB
D. CSMA/CS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The Carrier Sense Multiple Access - Collision Detection (CSMA/CD) contention method verifies that a channel is clear before transmitting, and stops transmitting data when it detects a collision on the channel in use.

Carrier Sense Multiple Access (CSMA)is the channel access mechanism used by Ethernet LANs. CSMA defines when and how to access the channel to transmit data. There are two variants of CSMA: CSMA with Collision Avoidance (CSMA/CA) and CSMA/CD.

With CSMA/CD, the transmitting station waits to detect channel traffic before sending the first packet over the channel. If the channel happens to be idle, the station transmits its packets. Despite the process of checking the channel before transmitting, it is still possible for two stations to transmitat once, resulting in collisions. If a collision occurs, the transmitting stations perform a retransmission. This retransmission uses a back-off algorithm by which a station waits for a random amount of time before retransmitting. As soon there is a collision on the network, the transmitting station stops transmitting and waits for a random interval of time before attempting the transmission again.

You should not select CSMA/CA. With Carrier Sense Multiple Access - Collision Avoidance (CSMA/CA), the transmitting station listens for a signal on the channel, then only transmits when the channel is idle. If the channel is busy, it waits a random amount of time before re-attempting transmission. CSMA/CA protocol is used in 802.11-based wireless LANs, while CSMA/CD is used in Ethernet LANs. Collisions are more often avoided with CSMA/CA than with CSMA/CD because sending stations signal non-sending stations to "wait" a

specific amount of time and then check for clearance again before sending. The cost of these mechanisms is reduced throughput.

CSMA/CB and CSMA/CS are invalid Ethernet contention methods, and are therefore incorrect options.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

References:
https://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1904.html#wp1024630

https://www.cisco.com/c/en/us/support/docs/interfaces-modules/port-adapters/12768-eth-collisions.html

https://www.cisco.com/en/US/tech/tk389/tk214/tk125/tsd_technology_support_sub-protocol_home.html

QUESTION 12
Which two modes are Cisco Internetwork Operating System (IOS) operating modes? (Choose two.)

A. User Privilegedmode
B. User EXEC mode
C. Local configuration mode
D. Global configuration mode
E. NVRAM monitor mode

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

User EXEC mode and global configuration mode are the Cisco IOS operating modes. The following list shows the Cisco IOS operating modes along with their description:

- User EXEC mode: The commands in this mode are used to enable connections to remote devices and change the terminal settings for a short duration. User EXEC commands also enable you to perform basic tests and view system information.
- Global configuration mode: The commands in this mode enable you to make changes to the entire system.
- Privileged EXEC mode: The commands in this mode are used to configure operating parameters. This mode also provides access to the remaining command modes.
- Interface configuration mode: The commands in this mode allow you to change the operation for interfaces such as serial or Ethernet ports.
- ROM monitor: The commands in this mode are used to perform low-level diagnostics.

All the other options are incorrect because they are not valid Cisco IOS operating modes.

To enter privileged EXEC mode, you must enter the command enable on the router. You will then be prompted for the enable password, if one has been created.

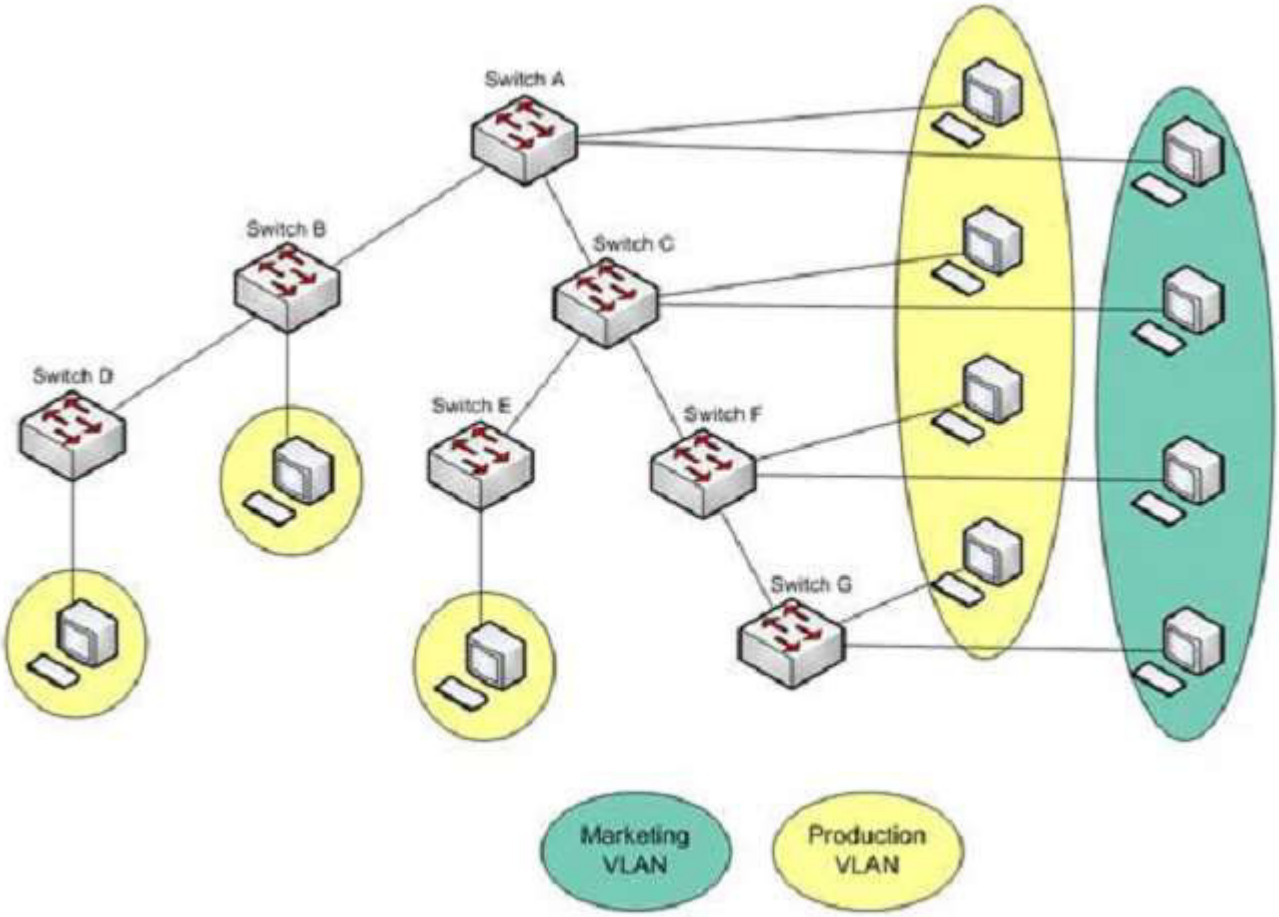
To enter global configuration mode, you must first enter privileged EXEC mode (see above) and then enter the command configure terminal (which can be abbreviated to config t), and the router will enter a mode that allows you to make global configuration changes.

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:
https://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/mgx_8850/software/mgx_r3/rpm/rpm_r1-1/configuration/guide/appc.html#wp1002608

QUESTION 13
You are a network administrator for your organization. Your organization has two Virtual LANs, named Marketing and Production. All switches in the network have both VLANs configured on them. Switches A, C, F, and G have user machines connected for both VLANs, whereas switches B, D, and E have user machines connected to the Production VLAN only. (Click the Exhibit(s) button to view the network diagram.)



To meet a new requirement, Marketing VLAN users must communicate with Production VLAN users and vice versa. What changes would be required for the network in this scenario?

A. Disable VTP pruning.
B. Convert all switch ports into trunk ports.
C. Create an access list with permit statements.
D. Install a routing device or enable Layer 3 routing on a switch.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

In this scenario, either a Layer 3 device or Layer 3 routing on a switch would be required to implement inter-VLAN routing. Although you could use multiple physical interfaces for the VLAN traffic, using trunk links between the switches and an external router would make more efficient use of the physical interfaces that you have. Only trunk links can carry traffic from multiple VLANs. These data frames must be frame tagged over the trunk link to identify the VLAN that sourced the frame. The receiving switch sees the VLAN ID, and uses this information to forward the frame appropriately. Additionally, the cables used to connect the router to the switches must be a straight-through cable and not a crossover cable.

When trunks links do not appear to be operating, it is always a good idea to make sure the port used for the trunk link is set as a trunk link and not as an access link. For example, the output below ofthe show interface fastethernet 0/15 switchport command indicates that Switch2 will not trunk because the port is set as an access link. This is shown in line 5 of the output:

<<output omitted>>
Switch2#show Interface fastethernet 0/15 switchport
Name: Fa0/15
SwitchportEnabled
Administrative Mode: access
Operational Mode: access
<<output omitted>>

The VLAN Trunking Protocol (VTP) pruning feature restricts unnecessarybroadcast traffic between multiple switches. It does not affect inter-VLAN traffic. Therefore, disabling VTP pruning will not permit inter-VLAN communication between the Marketing and Production VLANs.

Converting all switch ports into trunk ports will permit traffic from multiple VLANs to traverse over these links. However, traffic from one VLAN will be restricted to that VLAN only, and inter-VLAN communication will not be possible.

Access lists can permit or deny packets based on the packets' source/destination IP address, protocol, or port number. However, access lists can manipulate inter-VLAN traffic only when inter-VLAN traffic is enabled using a Layer 3 device or Layer 3 routing. Therefore, creating access lists will not enable inter-VLAN routing between the Marketing and Production VLANs.

Objective:
Network Fundamentals

Sub-Objective:
Describe the impact of infrastructure components in an enterprise network

References:

https://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/eos-eol-notice-listing.html

QUESTION 14
Which of the following methods will ensure that only one specific host can connect to port F0/1 on a switch? (Choose two. Each correct answer is a separate solution.)

A. Configure port security on F0/1 to forward traffic to a destination other than that of the MAC address of the host.
B. Configure the MAC address of the host as a static entry associated with port F0/1.
C. Configure port security on F0/1 to accept traffic only from the MAC address of the host.
D. Configure an inbound access control list on port F0/1 limiting traffic to the IP address of the host.
E. Configure port security on F0/1 to accept traffic other than that of the MAC address of the host.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To limit connections to a specific host, you should configure the MAC address of the host as a static entry associated with the port. Another solution would be to configure port security to accept traffic only from the MAC address of the host. By default, an unlimited number of MAC addresses can be learned on a single switch port, whether it is configured as an access port or a trunk port. Switch ports can be secured by defining one or more specific MAC addresses that should be allowed to connect, and by defining violation policies (such as disabling the port) to be enacted if additional hosts try to gain a connection.

The following example secures a switch port by manually defining the MAC address of allowed connections:

switch(config-if)# switchport port-security
switch(config-if)# switchport port-security mac-address 00C0.35F0.8301

The first command activates port security on the interface, while the second command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port.

Another approach to restricting a port to a single MAC address is to use the mac-address-table static command to assign a permanent MAC address to the port. The command below would assign the MAC address 0050.3e8d.62bb to port 15 on the switch:

switch(config)# mac-address-table static 0050.3e8d.6400 interface fastethernet0/15

In review, you can ensure that only a single MAC address can use a port by either of these two strategies:

- Configuring the MAC address as a static entry associated with the port
- Configuring portsecurity to reject traffic with a source address other than the desired MAC address

You should not configure port security on F0/1 to forward traffic to a destination other than that of the MAC address of the host. Traffic from other hosts should be rejected, not forwarded or accepted. For the same reason, you should not configure port security on F0/1 to accept traffic other than that of the MAC address of the host.

You cannot configure an inbound access control list on port F0/1 limiting traffic to the IP address of the host. It is impossible to filter traffic based on IP addresses on a Layer 2 switch.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot port security

References:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html#wp1070356

QUESTION 15
You are the network administrator for your company. You are in the process of verifying the configuration of the network devices to ensure smooth network connectivity. You want information on the routes taken by packets so that you are able to identify the network points where packets are getting dropped.

Which Cisco IOS command should you use to accomplish this task in the most efficient manner?

A. tracert

B. traceroute
C. extended ping
D. ping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You should use the traceroute command. The traceroute command finds the path a packet takes while being transmitted to a remote destination. It is also used to trackdown routing loops or errors in a network. The following code is a sample output of the traceroute command:

Type escape sequence to abort.
Tracing the route to 33.0.0.4

1 11.0.0.2 4 msec 4 msec 4 msec
2 24.0.0.3 20 msec 16 msec 16 msec
3 33.0.0.4 16 msec* 16 msec

Jan 20 16:42:48.611: IP: s=12.0.0.1 (local), d=33.0.0.4 (Serial0), len 28,
sending
Jan 20 16:42:48.615: UDP src=39911, dst=33434
Jan 20 16:42:48.635: IP: s=11.0.0.2 (Serial0), d=11.0.0.1 (Serial0), len 56,
rcvd 3
Jan 20 16:42:48.639: ICMPtype=11, code=0

The tracert command is incorrect because this command is used by Microsoft Windows operating systems, not the Cisco IOS command line interface. However, the purpose of the tracert command is similar to the Cisco traceroute utility, namely to test the connectivity or "reachability" of a network device or host. The tracert command uses Internet Control Message Protocol (ICMP).

The extended ping Cisco IOS command can be issued on a router to test connectivity between two remote routers. Thisoption is incorrect because you are not testing connectivity in this scenario; you want to determine the route a packet takes through the internetwork.

The ping command is also incorrect because you are not testing connectivity in this scenario; you want to determine the route a packet takes through the internetwork.

Objective:
Routing Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_t1.html#wp1065453

https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13730-ext-ping-trace.html

https://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1907.html

QUESTION 16
You have a router that is not syncing with its configured time source. Which of the following is NOT a potential reason for this problem?

A. The reported stratum of the time source is 12
B. The IP address configured for the time source is incorrect
C. NTP authentication is failing
D. There is an access list that blocks port 123

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A reported stratum of 12 will not cause a router's inability to synchronize with its configured time source. The stratum value describes the device's distance from the clock source, measured in NTPserver hops. When a router reports a stratum value over 15, it is considered unsynchronized. Therefore, a report of 12 could be normal.

The other options describe potential reasons for a lack of synchronization.

When you are configuring the local router with a time source, if the IP address configured for the time source is incorrect, then no synchronization will occur.

If NTP authentication is configured between the local router and its time source, and that process is failing (for example, due to a non-matching key or hashing algorithm), then synchronization will not occur.

If there were an access list applied to any interface in the path between the local router and its time source that blocks port 123 (the port used for NTP), then synchronization will not occur.

Objective:
Infrastructure Services

Sub-Objective:
Configure and verify NTP operating in client/server mode

References:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_management/7x/b_6k_System_Mgmt_Config_7x/configuring_ntp.html

QUESTION 17
Which media access control method is used by Ethernet technology to minimize collisions in the network?

A. CSMA/CD
B. token passing
C. back-on algorithm
D. full-duplex

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Carrier Sense Multiple Access - Collision Detection (CSMA/CD) is used by Ethernet technology to minimize collisions in the network. The CSMA/CD method uses a back-off algorithm to calculate random time for retransmission after a collision. When two stations start transmitting at the same time, their signals will collide.

The CSMA/CD method detects the collision, and both stations hold the retransmission for a certain amount of time that is determined by the back-off algorithm. This is an effort to help ensure that the retransmitted frames do not collide.

Token passing is used by the token-ring network topology to control communication on the network.

Full-duplex is the Ethernet communication mode that allows workstation to send and receive simultaneously. With the use of full-duplex, the bandwidth of the station can effectively be doubled. Hubs are not capable of handling full-duplex communication. You need dedicated switch ports to allow full-duplex communication.

The back-on algorithm is an invalid option. There is no such contention method.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

References:

http://docwiki.cisco.com/wiki/Ethernet_Technologies

QUESTION 18
Which Cisco IOS command is used on a Catalyst 2950 series switch to verify the port security configuration of a switch port?

A. show interfaces port-security
B. show port-securityinterface
C. show ip interface
D. show interfaces switchport

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show port-security interface command displays the current port security and status of a switch port, as in this sample output:

Switch# show port-security interfacefastethernet0/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 2
Total MAC Addresses: 2
Configured MAC Addresses: 2
Aging Time: 30 mins
Aging Type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0

The sample output indicates that port security has been enabled on interface FastEthernet0/1, and that a maximum of two MAC addresses have been configured. A violation policy of Shutdown indicates that if a third MAC address attempts to makea connection, the switch port will be disabled.

The violation mode setting has three possible values that take the following actions when a violation occurs:

- protect Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- restrict Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment. It will send a Syslog message and an SNMP trap as well.
- shutdown Puts the interface into the error-disabled state immediately and sends an SNMP trap notification

The show ip interface command is incorrect because it displays protocol-related information about an interface, and nothing pertaining to switch port security.

The show interfaces switchport command is incorrect because it displays non-security related switch port information, such as administrative and operational status and trunking.

The show interfaces port-security command is incorrect because this is not a valid Cisco command.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot port security

References:

QUESTION 19
What is the broadcast address for subnet 172.25.4.0/23?

A. 172.25.4.255
B. 172.25.5.255
C. 172.25.6.255
D. 172.25.7.255

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The broadcast address for subnet 172.25.4.0/23 will be 172.25.5.255.

When using a mask of /23, the subnet mask is 255.255.254.0. This means that the interval, or block size, of each subnet is 2, and that it will be incremented in the third octet. Therefore, the next network ID after 172.25.4.0 will be 172.25.6.0. Since the broadcast address of each subnet is the last address in that subnet before the next network ID, the broadcast address will be 172.25.5.255.

172.25.4.255 is a valid address in the 172.25.4.0/23 network, since the network range is 172.25.4.1 - 172.25.5.254.

172.25.6.255 is a valid address in the 172.25.6.0/23 network. Its range is 172.25.6.1 -172.25.7.254. Since the next network ID after 172.25.6.0 is 172.25.8.0, as the interval is 2 and it is incremented in the third octet, the broadcast address would be 172.25.7.255.

For the same reason, 172.25.6.255 is the broadcast address for the 172.25.6.0/24 network.

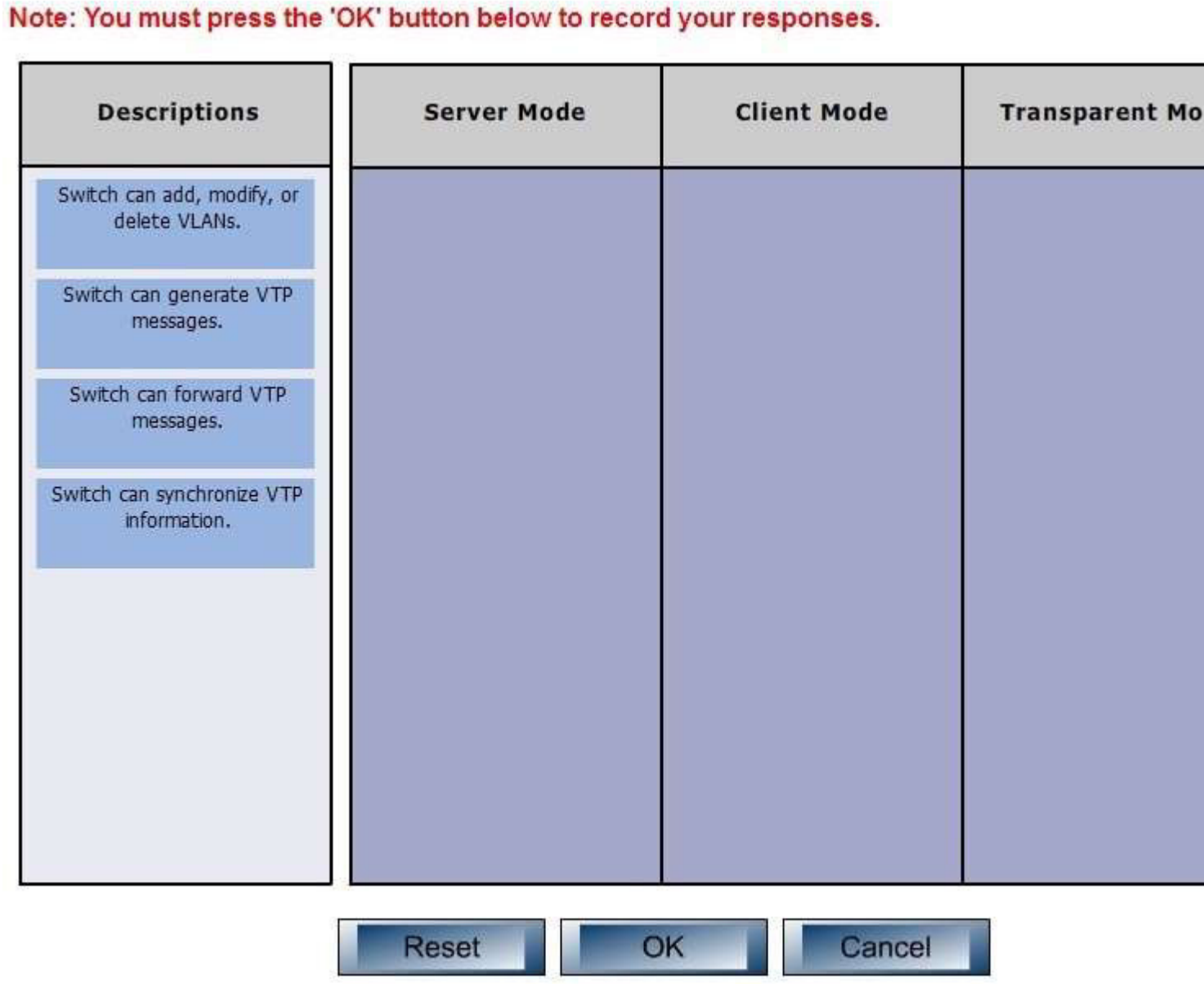
Objective:
Network Fundamentals

Sub-Objective:
Apply troubleshooting methodologies to resolve problems

References:
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html#ustand_ip_add

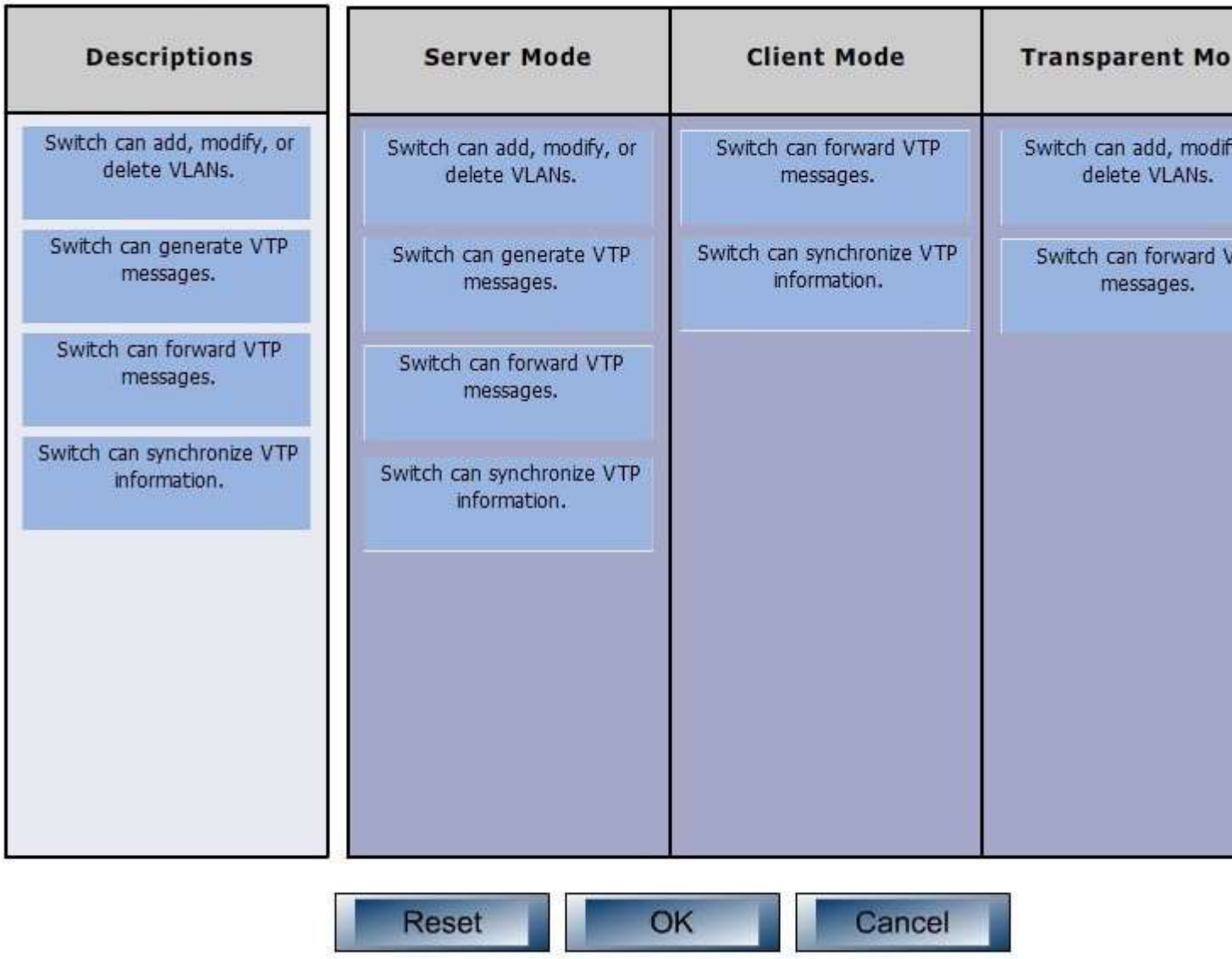
QUESTION 20
DRAG DROP
Click and drag the VLAN Trunking Protocol (VTP) mode descriptions on the left to their corresponding VTP modes on the right. (The descriptions on the left can be used more than once.)

Select and Place:



Correct Answer:

Note: You must press the 'OK' button below to record your responses.



Section: (none)
Explanation

Explanation/Reference:
Explanation:

VTP server mode is the default VTP mode.

VTP is a proprietary Cisco protocol used to share VLAN configuration information between Cisco switches on trunk connections. VTP allows switches to share and synchronize their VLAN information, which ensures that your network has a consistent VLAN configuration.

In VTP server mode:

- Switch can create, modify, or delete VLANs.
- Switches send/forward advertisements.
- Switches synchronize VTP information.
- VLAN information is saved in Non Volatile RAM (NVRAM).

In VTP Client mode:

- Switches forward advertisements.
- Switches synchronize VTP information.
- VLAN information is not saved in NVRAM.

In VTP Transparent mode:

- Switch can create, modify, or delete VLANs.
- Switches forward advertisements.
- Does not synchronize VTP information.
- VLAN information is saved in NVRAM.

Objective
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot VLANs (normal range) spanning multiple switches

References:

QUESTION 21
A new switch is added to the network, and several production VLANs are shut down. Which of the following is a probable cause for this scenario? (Choose two.)

A. The newswitch has a lower configuration revision number than existing switches.
B. The new switch has a higher configuration revision number than existing switches.
C. The new switch is operating in transparent mode.
D. The new switch is operating in server mode.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The VLAN database of the new switch will overwrite the VLAN databases of the production switches because it is operating in server mode and has a higher VLAN configuration revision number. The VLAN Trunking Protocol (VTP) is used to synchronize VLANs between different switches. The VTP configuration revision number is used to determine which VTP switch has the most current version of the VLAN database, and is incremented whenever a VLAN change is made on a VTP server switch. The show vtp status command is used to view the configuration revision number, as shown in this sample output:

Switch# show vtp status
VTP Version : 2
Configuration Revision : 62
Maximum VLANs supported locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Server
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled

VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80

This switch has a configuration revision number of 62, which will be compared to other switches in the same VTP domain. If the production switches have a lower configuration revision number than the new switch, their VLAN databases will be replaced with the VLAN database of the new switch. This could mean that VLANs that formerly existed on those production switches may be deleted. Any switch ports that had been assigned to VLANs that become deleted will be disabled, possibly resulting in catastrophic network failure. All VTP switches in the same VTP domain should have a domain password defined, which will protect against a rogue switch being added to the network and causing VLAN database corruption.

The new switch does not have a lower configuration revision number, since this would cause the new switch to have its VLAN database replaced with the existing production VLANs. This would not cause the problem described in the scenario.

The new switch is not operating in transparent VTP mode because a switch operating in transparent VTP mode will never synchronize its VLAN database with other switches.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot VLANs (normal range) spanning multiple switches

References:

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25sg/configuration/guide/conf/vlans.html

QUESTION 22
Which of the following splits the network into separate broadcast domains?

A. bridges
B. VLANs
C. switches
D. hubs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Virtual LANs (VLANs) split the network into separate broadcast domains, as would a router. VLANs are a software implementation embedded in a switch's software that allows the switch's hardware to switch packets only to ports that belong to the same VLAN.

Neither a switch nor a bridge splits the network into separate broadcast domains. Both a switch and a bridge are used to create collision domains for each connected node. Collision domains confine traffic destined to or coming from a particular host to the switch port of that node in the switch. This reduces collisions, which in turn decreases retransmissions and elevates throughput. Switches work at Layer 2 in the OSI model and perform the function of separating collision domains. Neither switches nor bridges filter broadcasts and distribute them across all ports.

A hub does not split the network into separate broadcast domains. A hub regenerates signal when it passes through its ports, which means that it acts as a repeater and port concentrator only. Hubs and repeaters are

Layer 1 devices that can be used to enlarge the area covered by a single LAN segment, but cannot be used to segment the LAN as they have no intelligence with regards to either MAC addresses or IP addresses. Hubs provide a common connection point for network devices, and connect different network segments. Hubs are generally used for LAN segmentation. Hubs work at Layer 1 of the OSI model, which is the physical layer. Hubs do not filter broadcasts or create collision domains.

Objective:
Network Fundamentals

Sub-Objective:
Describe the impact of infrastructure components in an enterprise network

References:

http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_LAN_Switching#LAN_Switching

QUESTION 23
Which commands would you use to determine the IP address and hostname of a directly connected switch from which you received VLAN information? (Choose two. Each correct answer is part of the solution.)

A. show vtp status
B. show cdp neighbors detail
C. show cdp neighbor status
D. show vtp counters
E. show cdp neighbor

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The VLAN Trunking Protocol (VTP) is used to synchronize VLANs between switches, and the question implies that VTP is being used in this environment. The show vtp status command will display the IP address ofthe switch that last updated your VLAN database. The output of this command is as follows:

Switch# show vtp status
VTP Version : 2
Configuration Revision : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs : 33
VTP Operating Mode :Server
VTP Domain Name : Lab_Network
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 10.1.1.2 at 8-12-99 15:04:49
<output omitted>

The "Configuration last modified by 10.1.1.2" output reveals the IP address of the switch from which you received VLAN information. Once you know the IP address of the switch, you can use the show cdp neighbors detail command to determine the hostname associated with this IP address. The output of this command is as follows:

switch# show cdp neighbors detail
Device ID: RouterB
Entry address(es):

IP address: 172.20.52.254
Platform: cisco 2621, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 120 sec
<<output omitted>>

Device ID: SwitchB
Entry address(es):
IP address: 10.1.1.2
Platform: cisco WS-C2950G-24, Capabilities: Switch IGMP
Interface: FastEthernet0/4, PortID (outgoing port): FastEthernet0/24
Holdtime: 101 sec
<<output omitted>>

The show cdp neighbors detail command provides detailed information about directly connected Cisco devices. The detail option is required to provide the IP address of the neighboring devices, and indicates here that IP address 10.1.1.2 is assigned to Device ID: SwitchB, which is the hostname for this device. SwitchB is the switch from which you received VLANs.

Although not offered as an option, the show cdp entry* command will also display all directly connected devices and will indicate the hostname and the IP address and platform, but will not indicate from which device VTP information was received. Its output is shown below:

switch#show cdp entry*

Device ID: SwitchB
Entry address(es):
IP address: 10.1.1.2
Platform: cisco WS-C2950G-24, Capabilities: Switch IGMP
Interface: FastEthernet0/4, Port ID (outgoing port): FastEthernet0/24
Holdtime: 101 sec
<<output omitted>>
This command displays the same information as the show cdp neighbor detail command. It includes:

- The IP address of the neighbor (in this case 10.1.1.2)
- The port on which the CDP information was received (in this case FastEthernet0/4)
- The platform (in this case a Cisco WS-C2950G-24 Switch)

The show vtp counters command is incorrect because it does not display information about neighboring devices, nor information regarding from which switch VLANs were received.

The show cdp neighbor command is incorrect because the detail option is required to display the IP addresses of neighboring devices.

The show cdp neighbor status command is incorrect because this is not a valid Cisco IOS command.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot VLANs (normal range) spanning multiple switches

References:

https://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

https://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/eos-eol-notice-listing.html

QUESTION 24
You wish to configure Secure Shell (SSH) support on your router so that incoming VTY connections are secure. Which of the following commands must be configured? (Choose all that apply.)

A. ip domain-name
B. transport input ssh
C. ip access-group
D. crypto key generate rsa
E. service config

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Secure Shell (SSH) provides a secure alternative to Telnet for remote management of a Cisco device. Configuring Secure Shell (SSH) support on a Cisco router involves a minimum of three commands:

- ip domain-name [domain-name]: configures the DNS of the router (global configuration mode)
- crypto key generate rsa: generates a cryptographic key to be used with SSH (global configuration mode)
- transport input ssh: allows SSH connections on the router's VTY lines (VTY line configuration mode)

The transportinput ssh command allows only SSH connectivity to the router, and prevents clear-text Telnet connections. To enable both SSH and Telnet, you would use the transport input ssh telnet command.

The ip access-group command is incorrect because this command is used to activate an access control list (ACL) on an interface, and does not pertain to SSH.

The service config command is incorrect because this command is used to automatically configure routers from a network server, and does not pertain to SSH.

Objective:
Network Fundamentals

Sub-Objective:
Select the appropriate cabling type based on implementation requirements

References:

https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

QUESTION 25
You have a class C address range and are planning a network that has an average of 50 hosts per subnet.

How many host bits will have to be borrowed for subnetting so that the maximum number of subnets can be implemented?

A. 1
B. 2
C. 3
D. 4
E. 6

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

A class C address has 8 bits in host space. By using 2 bits from the host space for subnetting, leaving 6 host bits, you can create subnets that can accommodate up to 62 hosts each (26- 2 = 62). This will ensure that the requirement of 50 hosts per subnet is met and the maximum number of subnets is provided.

The formulas to calculate the number of subnets and hosts are:

Number of subnets = 2number-of-subnet-bits
Number of hosts per subnet = 2number-of-host-bits- 2

If you take 1 bit for subnetting:
Number of subnets = 21= 2
Number of hosts per subnet = 27- 2 = 126

This results in a mask of 255.255.255.128 or /25. Since each subnet need not be bigger than 50, this solution would not maximize the number of subnets.

If you take 2 bits for subnetting:
Number of subnets = 22= 4
Number of hosts per subnet = 26- 2 = 62

This results in a mask of 255.255.255.192 or /26. This solution would create more subnets, but the subnets are smaller than the requirement.

If you take 3 bits for subnetting:
Number of subnets = 23= 8
Number of hosts per subnet = 25- 2 = 30

This results in a mask of 255.255.255.224 or /27. This would create more subnets, but the subnets are smaller than the requirement.

If you take 4 bits for subnetting:
Number of subnets = 24= 16
Number of hosts per subnet = 24- 2 = 14

This results in a mask of 255.255.255.240 or /28. This solution would create more subnets, but the subnets are smaller than the requirement.

If you take 6 bits for subnetting:
Number of subnets = 26= 64
Number of hosts per subnet = 22- 2 = 2

This mask, 255.255.255.252 or /30, yields only 2 IP addresses, but is quite commonly used on a point-to-point link, such as between two routers. This solution would create more subnets, but the subnets are smaller than the requirement.

You will always subtract 2 from the number of hosts (the formula of 2number-of-host-bits- 2) because the all-zeros bit address is reserved for the network address and the all-ones bit address is reserved for the broadcast address.

Prior to Cisco IOS Software Release 12.0, it was common practice to subtract 2 from the networks formula (2number-of-subnet-bits) to exclude addresses of all 1s and all 0s (called the all-ones subnet and subnet zero). Today that range is usable,except with some legacy systems. On certain networks with legacy software, you may need to use the previous formula (2n- 2) to calculate the number of subnets.

Objective:
Network Fundamentals

Sub-Objective:
Apply troubleshooting methodologies to resolve problems

References:
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html#ustand_ip_add

https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/13711-40.html

QUESTION 26
On a Cisco 2950 switch, which status LED and color combination indicates a Power On Self Test (POST) failure?

A. system LED: no color
B. system LED: solid red
C. system LED:solid amber
D. stat LED: no color
E. stat LED: green

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A POST failure is indicated by a solid amber color on the system LED. The switch automatically runs POST which is a series of self-tests to verify proper functioning, after the power is connected. The system LED is off (no color) at the time that POST begins. The LED will turn green if POST is successful, or it will turn amber if POST fails.

The system LED will not be colorless. The system LED will show no color at the beginning of the POST cycle, not after a POST failure.

The system LED will not be solid red after a POST failure. Cisco LEDs do not have a red color mode.

The Stat LED indicates the status of each port. If it is amber there is a signal but the port is not forwarding, either because of an address violation or it has been disabled. If it is colorless, there is no signal. In this case:

- Ensure the switch has power
- Ensure the proper cable type is in use (for a switch to switch connection use a crossover cable: for a switch to host and or switch to router connection use a straight through)
- Ensure a good connection by reseating all cables

If it is green, the port has a signal and is functional. Green means

- Layer 1 media is functioning between the switch and the device on the other end of the cable
- Layer 2 communication has been established between the switch and the device on the other end of the cable

LED color	Status
Off	RPS is either shut down or not installed.
Solid Green	RPS is installed and operational.
Blinking Green	Another switch in the stack is being backed up by RPS.
Solid Amber	Standby mode. It should turn green after pressing the active/standby button on the RPS. If it does not turn green, the RPS power supply or FAN might have failed.
Blinking Amber	Switch internal power supply is down and the switch is functioning on RPS.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshootinterswitch connectivity

References:

QUESTION 27
Which command is used to disable Cisco Discovery Protocol (CDP) on a Cisco router?

A. disable cdp
B. no cdp run
C. no cdp enable
D. no cdp advertise-v2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The nocdp run command is used to disable CDP on a Cisco router globally. CDP is a Layer 2 (Data Link layer) protocol that discovers information about neighboring network devices. CDP does not use network layer protocols to transmit information because it operates at the Data Link layer. Therefore, it is useful to determine information about directly connected Cisco network devices, because it can operate when network protocols have not been configured or are misconfigured. The show cdp neighbors detail command is used to view the IP addresses of the directly connected Cisco devices.

The no cdp advertise-v2 command disables CDPv2 advertisements. It will not disable the protocol globally.

The no cdp enable command is used to disable CDP on an interface. In a situation where CDP needs to be disabled on a single interface only, such as the interface leading to the Internet, this command would be executed from interface configuration mode for that specific interface. It will not disable the protocol globally. For example, to disable CDP for only the serial0 interface, the command sequence would be:

Router#configure terminal
Router(config)#interface serial 0
Router(config-if)no cdp enable

The disable cdp command is not a valid Cisco command.

Objective:

LAN SwitchingFundamentals

Sub-Objective:
Configure and verify Layer 2 protocols

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html#wp1074517

QUESTION 28
In the following partial output of the show ip route command, what does the letter D stand for?

D 192.1.2.0/24 via 5.1.1.71 [w:0 m:0]

C 192.8.1.1/32 directly connected to loopback 0

A. This is a default route
B. This is an EIGRP route
C. This is static route
D. This is a directly connected route

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The letter D indicates that it was a route learned by the EIGRP routing protocol. In the output of the show ip route command, each route will have a letter next to it that indicates the method by which the route was learned. At the beginning of the output will be a legend describing the letters as shown below:

Router# show ip route
Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
C - connected, S - static, E - EGP derived, B - BGP derived,
* - candidate default route, IA - OSPF inter area route,
i - IS-IS derived, ia - IS-IS, U - per-user static route,
o - on-demandrouting, M - mobile, P - periodic downloaded static route,
D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route

The letter does not indicate that it is a default route. The default route (if configured) will appear at the end of the legend as follows:

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

The letter does not indicate that it is a static route. Static routes will have an "S" next to them.

The letter does not indicate that it is a directly connected route. Directly connected routes will have a "C" next to them.

Objective:
Routing Fundamentals

Sub-Objective:
Interpret the components of routing table

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/command/iri-cr-book/iri-cr-s1.html#wp2136320492

QUESTION 29
You are the network administrator for your company. You want to use both IPv6 and IPv4 applications in the network. You also want to ensure that routers can route both IPv6 and IPv4 packets.

Which deployment model should be implemented to accomplish the task?

A. IPv6 over IPv4 tunnels
B. IPv6 over dedicated Wide Area Network (WAN) links
C. Dual-Stack Backbones
D. Protocol translation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A dual-stack backbone deployment model should be used to accomplish the task in this scenario. When routers route both IPv6 and IPv4 packets, it is called dual stack routing or a dual-stack backbone.

The following deployment models are available for IPv4 to IPv6 migration:

- IPv6 over IPv4tunnels: IPv6 traffic is encapsulated into IPv4 packets. Then these packets are transferred over an IPv4 WAN. This model eliminates the need to create separate circuits to connect to the IPv6 networks. This model increases protocol overhead because of the IPv6 headers and requires one end to be capable of both protocols
- Protocol translation: A translation method of allowing an IPv6 host to communicate with an IPv4 host. This is accomplished with the help of Network Address Translation - Protocol Translation (NAT-PT) used to configure translation between IPv6 and IPv4 hosts. NAT-PT allows communication between IPv6 hosts and applications, and native IPv4 hosts and applications.
- IPv6 over dedicated WAN links: A new deployment of IPv6 is created. In this model, IPv6 hierarchy, addressing, and protocols are used by all nodes. However, this model involves cost for creating IPv6 WAN circuits. This solution is not designed for LAN translation but rather translation over WAN links.
- Dual-Stack Backbones: A hybrid model in which backbone routers have dual-stack functionality, which enables them to route both IPv4 and IPv6 packets. It is suitable for an enterprise that uses both IPv4 and IPv6 applications. Running IPv6 and IPv4 together in a network is known as dual-stack routing.

Objective:
Network Fundamentals

Sub-Objective:
Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

References:

https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPV6at_a_glance_c45-625859.pdf

https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6/25156-ipv6tunnel.html#intro

QUESTION 30
Which statements are TRUE regarding Internet Protocol version 6 (IPv6) addresses? (Choose three.)

A. An IPv6 address is divided into eight 16-bit groups.
B. A double colon (::) can only be used once in a single IPv6 address.
C. IPv6 addresses are 196 bits in length.

D. Leading zeros cannot be omitted in an IPv6 address.
E. Groups with a value of 0 can be represented with a single 0 in IPv6 address.

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

IPv6 addresses are divided into eight 16-bit groups, a double colon (::) can only be used once in an IPv6 address, and groups with a value of 0 can be represented with a single 0 in an IPv6 address.

The following statements are also true regarding IPv6 address:

- IPv6 addresses are 128 bits in length.
- Eight 16-bit groups are divided by a colon (:).
- Multiple consecutive groups of 16-bit 0s can be represented with double colon (::) (only once)
- Double colons (::) represent only 0s.
- Leading zeros can be omitted in an IPv6 address.

The option stating that IPv6 addresses are 196 bits in length is incorrect. IPv6 addresses are 128 bits in length.

The option stating that leading zeros cannot be omitted in an IPv6 address is incorrect. Leading zeros can be omitted in an IPv6 address.

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast IPv6 address types

References:
http://docwiki.cisco.com/wiki/IPv6

QUESTION 31
Which of the following features is used with the ip nat inside command to translate multiple devices in the internal network to the single address in the IP address pool?

A. static
B. override
C. overload
D. dynamic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The overload keyword, when specified with the ip nat inside command, translates multiple devices in the internal network to a single address in the IP address pool.

For example:

ip nat pool test 172.28.15.1 172.28.15.1 prefix 24

In this example, the NAT pool named "test" only has a range of one address. Another variation of this command is as follows:

ip nat inside source list 3 interface serial 0 overload

This command configures NAT to overload on the address assigned to the serial 0 interface.

When this variation is used, the command uses a list named 3 to determine the addresses in the pool

With static NAT, translation mappings are created statically and are placed in the translation tables regardless of whether there is traffic flowing.

With dynamic NAT, the translation mappings table is populated as the required traffic flows through NAT-enabled devices.

Override is not a valid NAT option. There is no such option.

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot inside source NAT

References:
https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html#topic1

QUESTION 32
You are configuring the link between a Cisco 2950 series switch and a Cisco 2611 router. You have physically connected the router's Ethernet port to the switch using a straight-through cable. The switch has not been configured, except for a hostname. The router's hostname has also been configured, and the Ethernet port has been enabled. However, you forgot to assign an IP address to the Ethernet port.

You issue the show cdp neighbors command and get the following output:

```
RouterA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID    Local Interface     Holdtime    Capability  Platform  Port
ID
SwitchA      Eth 0/0           157             S      2950      Fas 0/0
```

If you did not configure IP addresses, how is this information being passed between the two devices?

A. The devices established a connection using default IP addresses.
B. The ip unnumbered command has been issued, which means the interface does not require an IP address to be configured.
C. CDP is a Layer 2protocol and does not require IP addresses to be configured.
D. CDP uses its own IP addressing system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

CDP is a Layer 2 protocol and does not require IP addresses to be configured. The structure of the OSI model requires that the upper-layer protocols rely on the lower-layer protocols for operation. Protocols at Layer 3 cannot be operational unless Layers 1 and 2 are operational. Conversely, lower-layer protocols do not rely on

upper-layer protocols for their operation. Because CDPoperates at Layer 2 of the OSI model, it does not require an IP address to be active, since IP addresses are a function of Layer 3.

The ip unnumbered command has not been issued in this scenario. This command can only be used on serial interfaces, not Ethernet interfaces. It allows a serial interface to use an address that is already applied to an Ethernet interface.

Information is not being passed between the devices through default IP addresses. There is no such thing as default IP addresses on Ethernet interfaces for Cisco routers.

Information is not being passed between the devices through CDP's IP addressing system. CDP does not have its own IP addressing system because it does not use IP addresses for its operation.

Objective:
InfrastructureMaintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html#wp1074517

QUESTION 33
Which three statements are TRUE regarding a Local Area Network (LAN)? (Choose three.)

A. A LANis confined to one building or campus.
B. A LAN can cover great distances.
C. A LAN provides fast data transmission.
D. A LAN is easily expandable.
E. LANs require the use of a router to communicate between local hosts.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

ALAN is confined to one building or campus, provides fast data transmission, and is easily expandable. A LAN refers to the interconnection of computers within a building or a group of buildings. A LAN generally uses twisted pair cables for data transmission.

The following are some characteristics of LANs:

- LANs are generally confined to a building, a group of buildings, or a campus.
- Every computer in the LAN can communicate with every other computer on the network.
- A LAN is easy to set up, as physical connectivity can be easily established.
- The cost of the transmission medium used is low, as a LAN generally uses CAT5, CAT5e, or CAT6 cables for data transmission.
- A LAN provides fast data transmission rates.

The option stating that a LAN can cover great distances is incorrect. A Wide Area Network (WAN) is a network that does not have any geographical boundaries. The Internet is the best example of a WAN.

LANs do not require the use of a router to communicate (although they can be used to connect subnets) between local hosts. Hosts can communicate through a hub or switch.

Objective:

Network Fundamentals

Sub-Objective:
Compare and contrast network topologies

References:

http://docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols

QUESTION 34
Which type of Category 5 unshielded twisted-pair (UTP) cable is used to work as a trunk between two switches?

A. RJ-45 straight-through
B. RJ-41 crossover
C. RJ-11 straight-through
D. RJ-45 crossover

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

An RJ-45 crossover cable connects two switches. To act as a trunk a trunking protocol such as ISL or 802.1q must be configured on the link. . A trunk is a connection between two switches that is used to carry traffic from multiple VLANs.

In general, the rule to follow when choosing between a straight-through and a crossover cable is:

- When connecting like devices (i.e. router to router, switch to switch), use a crossover cable.
- When connecting dissimilar devices (i.e. switch to router), use a straight-through cable.

The one exception to this rule is when connecting a computer NIC to a router, in which case a crossover cable is used. Be aware, however, that many devices, including network cards in computers, now have the ability to sense automatically when they are connected to a like device and adapt to the connection, making crossover cables unnecessary in those situations.

You should not choose an RJ-45 straight-through cable. The cable type to be used depends on the circuit connection of the hardware. To connect two switches, a crossover cable is required. The difference between a straight-through cable and a crossover cable lies in the location of the wire termination on the two ends of an RJ-45 cable. If the UTP cable wire connects Pin 1 of one side to Pin 1 of other side and Pin 2 to 2 through all eight pins of the RJ 45 connector, the cable is said to be straight-through. On the other hand, if Pin 1 of one side of an RJ-45 cable connects to Pin 3 of the other end, and Pin 2 connects to Pin 6 of the other end, it is known as a crossover cable. A straight-through cable is used to connect a computer's network interface card (NIC) to a hub or switch.

You should not choose an RJ-41 crossover cable. RJ-41is a single-line universal data jack normally associated with fixed-loss loop (FLL) or programmed (P) modems. It is not used between switches.

You should not choose an RJ-11 straight-through cable type. RJ-11 UTP cables have four pins and are used to connect voice instruments. RJ-11 UTP cables are not intended for connecting computers and transferring data. They are commonly used for telephones and modems.

Note: Cisco switches have an auto-mdix feature that notices when the wrong cabling pinouts are used,and readjusts the switch's logic so that the cable will work.

Objective:

Network Fundamentals

Sub-Objective:
Select the appropriate cabling type based on implementation requirements

References:

http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Designing_Switched_LAN_Internetworks#Designing_Switched_LAN_Internetworks

https://www.cisco.com/c/en/us/support/docs/routers/7000-series-routers/12223-14.html#topic4

QUESTION 35
Which of the following statements are TRUE regarding the following output? (Choose all that apply.)

```
Router# show ip route

Gateway of last resort is 192.168.15.1 to network 0.0.0.0

<<output omitted>>
D 192.168.10.0 [90/2172416] via 192.168.15.254, 0:01:42, Serial0/1/0
C 192.168.14.0 is directly connected, Serial0/0/0
D 192.168.52.0 [90/2172416] via 192.168.15.254, 0:00:35, Serial0/1/0
[90/2172416] via 192.168.15.5, 0:02:05, Serial0/0/0
C 192.168.15.0 is directly connected, Serial0/1/0
C 192.168.20.0 is directly connected, Serial0/0/1
S 192.168.50.0 [1/0] via 192.168.53.1
C 192.168.33.0 is directly connected, Loopback1
D 192.168.25.0 [90/2196545] via 192.168.20.254, 0:01:20, Serial0/0/1
```

A. There are four default routes on this router.
B. There are four physically connected interfaces on this router.
C. This router is running EIGRP.
D. The metric for the routes learned via a routing protocol is 90.
E. A packet for the 192.168.52.0 network will be load-balanced across two paths.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

This router is running EIGRP and a packet for the 192.168.52.0 network will be load-balanced across two paths.

EIGRP routes display with a D code in the leftmost column of the show ip route command. The D stands for Diffusing Update Algorithm (DUAL), which is the algorithm used by EIGRP to determine the best and potential backup paths to each remote network. There are four EIGRP-learned routes in this exhibit.

When two routes with equal metrics exist in the routing table, EIGRP will send packets using both paths. In the output there are two routes listed for the 192.168.52.0 network. Both have the same metric value (2172416). Therefore, packets will be sent to that network via the Serial 0/1/0 interface to the neighbor at 192.168.15.254 and via the Serial 0/0/0 interface to the neighbor at 192.168.15.5. Both paths, either directly or indirectly, lead to the 192.168.52.0 network, and both paths have the same cost.

There are not four default routes on this router. The D represents EIGRP-learned routes, not default routes. There is one default route, as indicated by the line of output that says Gateway of last resort is 192.168.15.1 to network 0.0.0.0. Because Serial0/1/0 is directly connected to the 192.168.15.0 network, packets that are destined for networks not found in the routing table will be sent out on that interface.

The C in the leftmost column of the show ip route command represents directly connected networks, of which there are four in the exhibit. Closer examination, however, reveals that one of these entries (for network 192.168.33.0) is connected to a loopback interface (Loopback1), as opposed to a physical interface:

C 192.168.33.0 is directly connected, Loopback1

Loopback interfaces are virtual, software interfaces that appear in the routing table, but do not represent a physical interface on the router. Therefore, there are three physically connected interfaces on this router, not four.

The metric for the routes learned via a routing protocol is not 90. The 90 in the scenario output is the administrative distance (AD) of the route, and the 2196545 is the metric value (see below):

D 192.168.25.0 [90/2196545] via 192.168.20.254, 0:01:20, Serial0/0/1

Objective:
Routing Fundamentals

Sub-Objective:
Interpret the components of routing table

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book.html

QUESTION 36
Which of these applications uses the IMAP protocol to transfer information between a server and a host?

A. E-mail
B. FTP
C. Web browser
D. Telnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

E-mail applications use Internet Message Access Protocol (IMAP) to retrieve messages from mail servers. IMAP differs from Post Office Protocol (POP3) in that IMAP allows the manipulation of email message as they remain on the email server, unlike POP3 in which the email can only be downloaded to the client. By default, IMAP uses TCP port 143. IMAP3 uses port 220.

File Transfer Protocol (FTP) does not use IMAP. FTP transfers files from an FTP server to a client computer over the Internet or intranet. By default, FTP uses TCP port 21 to connect to the client system.

A Web browser does not use IMAP. It uses Hyper Text Transmission Control Protocol (HTTP) to exchange information over the Internet. A Web browser provides access to the Internet through which a user can access text, images, and other information on a Web site. By default, HTTP uses TCP port 80 to connect to the client computer.

Telnet does not use IMAP. Telnet is an application that remotely accesses a computer for the purpose of

executing commands. It uses TCP port 23 to connect to the remote computer.

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast TCP and UDP protocols

References:

http://docwiki.cisco.com/wiki/Internetworking_Basics#Multiplexing_Basicshttp://docwiki.cisco.com/wiki/Internetworking_Basics

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_protocol_cbac_fw/configuration/12-4/sec-prot-cbac-fw-12-4-book/sec-prot-email-insp.html

QUESTION 37
Which of the following is the wildcard (inverse) version of a /27 mask?

A. 0.0.0.7
B. 0.0.0.15
C. 0.0.0.31
D. 0.0.0.63E 0.0.31.255

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Wildcard masks (also known as inverse masks) are used within access control lists and OSPF network statements to identify a range of IP addresses. The wildcard mask specifies how many bits in the IP address must be examined to consider the IP address a "match" for the condition. A zero bit in the wildcard mask indicates a bit that should be examined in the IP address, while a one bit indicates a wildcard, or a bit in the IP address, that should not be examined. A /27 mask indicates that 27 bits (out of a total of 32 bits in an IPv4 address) are being used for network routing information, as follows:

11111111.11111111.11111111.11100000 (27 one bits, or /27)

To find the wildcard(inverse) version of this mask, the zero and one bits are simply reversed as follows:

11111111.11111111.11111111.11100000 (27 one bits, or /27)
00000000.00000000.00000000.00011111 (wildcard/inverse mask)

Converting this binary string back into decimalyields 0.0.0.31, which is the wildcard version of a /27 mask.

A much easier and faster way to determine a wildcard mask is to perform the following operations:

1. Put the regular mask in dotted decimal format -- in this case, /27 is 255.255.255.224
2. Subtract the value of the last octet from 255 -- in this case, 255 - 224 = 31
3. Set all other octets to 0, yielding a wildcard mask of 0.0.0.31

The remaining answers are incorrect, as they are wildcard versions of different masks as follows:

0.0.0.7 = /29 (or 255.255.255.248)
0.0.0.15 = /28 (or 255.255.255.240)
0.0.0.63 = /26 (or 255.255.255.192)
0.0.31.255=/19 (or 255.255.224.0)

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces

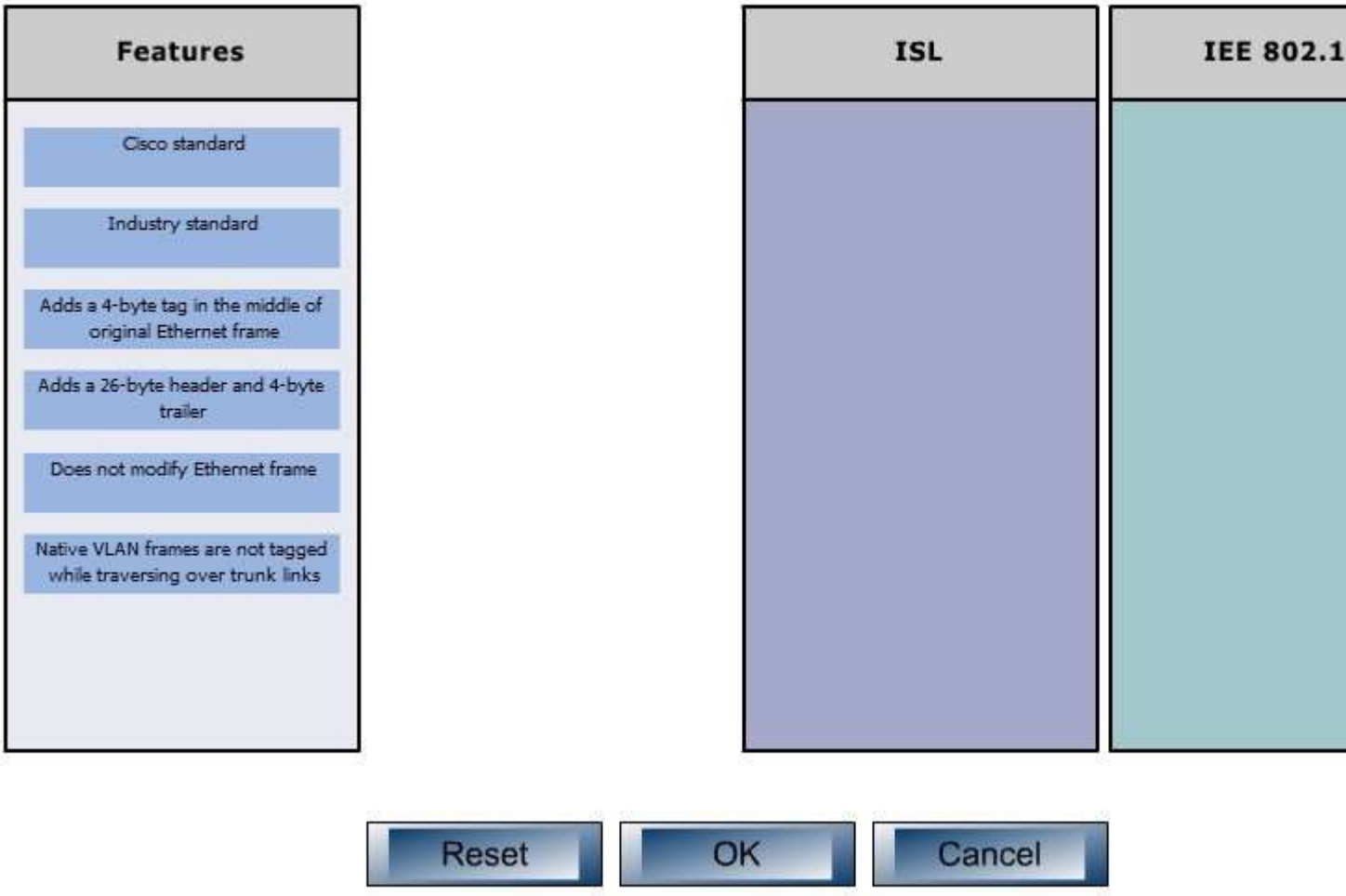
References:

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#topic2

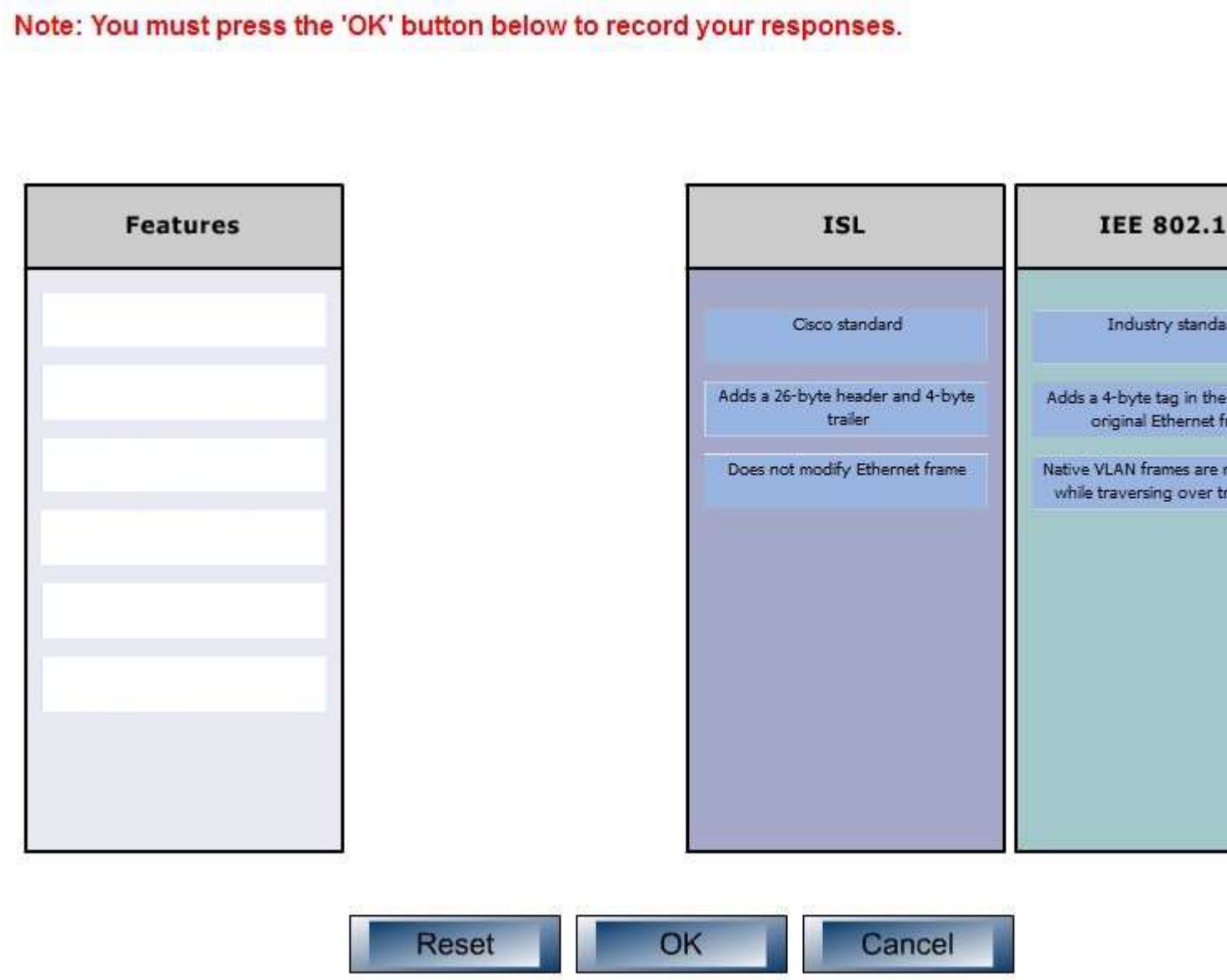
QUESTION 38
DRAG DROP
Click and drag the features on the left to their corresponding frame tagging method on the right.

Select and Place:

Note: You must press the 'OK' button below to record your responses.



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Explanation:

ISL and IEEE 802.1Q are VLAN frame tagging methods.
ISL:

- Is Cisco proprietary
- Adds a 26-byte header and4-byte trailer
- Does not modify Ethernet frame

IEEE 802.1Q frame tagging method:

- Is a standard method
- Adds a 4-byte tag in the middle of original Ethernet frame
- Has a concept called native VLAN. Native VLAN frames are not tagged while traversingover a trunk link.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot interswitch connectivity

References:

https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html#topic1

QUESTION 39
Which Cisco 2950 switch command or set of commands would be used to create a Virtual LAN (VLAN) named MARKETING with a VLAN number of 25?

A. switch(config)# vtp domain MARKETING 25
B. switch(config)# vlan 25switch(config-vlan)# name MARKETING
C. switch(config-if)# vlan 25 name MARKETING
D. switch(config)# vtp 25switch(config-vtp)# name MARKETING

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following commands would create a VLAN named MARKETING with a VLAN number of 25:

switch(config)# vlan 25
switch(config-vlan)# name MARKETING

The steps to add anew VLAN are as follows:

1. Create the new VLAN
2. Name the VLAN
3. Add the desired ports to the VLAN

VLANs on current Cisco switches are configured in global configuration mode. The VLAN is first created with the vlan # command, and then optionally named with the name vlan-name command. Interfaces are added to VLANs using either the interface or interface range commands.

The switch(config)# vtp domain MARKETING 25 command will not create a VLAN. This command creates a VLAN Trunking Protocol (VTP) domain. VTP is a means of synchronizing VLANs between switches, not a method of manually creating VLANs.

The vlan 25 name command is deprecated, and is not supported on newer Cisco switches. Even on switches that support the command, this answer is incorrect because the vlan 25 name command was issued in VLAN database mode, rather than interface mode.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot VLANs (normal range) spanning multiple switches

References:

https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html

QUESTION 40
Which command is used on a Catalyst 2950 series switch to enable basic port security on the interface?

A. set port-security
B. switchport port-security
C. set port-security enable
D. switchport port-security enable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The switchport port-security command is an interface configuration command used on a Catalyst 2950 series switch to enable basic port security on the interface. The syntax of the command is as follows:

switch(config-if)#switchport port-security

Switchport security can be used to:

- Limit the computers that are allowed to connect to the LAN (by specifying the MAC addresses allowed on the port)
- Limit the number of MAC address allowed to be accessing a port
- Set the action the port will take when a violation of the security rule occurs

The set port-security, set port-security enable, and switchport port-security enable commands are incorrect because these are not valid Cisco IOS commands.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot port security

References:
Page Not Found

QUESTION 41
What filtering criteria does a standard IP access list use to filter packets?

A. Layer 4 protocol in use
B. source IP address of the packets
C. destination IP address of the packets and Layer 4 protocol
D. IP address of the router on which access list is applied

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Access lists are sequential lists of permit or deny statements that filter traffic going through the router. Standard IP access lists filter network traffic based on the source IP address in a packet. You can create a standard IP access list by assigning access list numbers from 1 - 99 or 1300 - 1999 (expanded standard range). The expanded range is new set of numbers that can also be used for standard access lists.

The following command syntax shows a standard access list, with access list number 15 and IP address of the host to be denied (filtered) 192.168.144.2:

RouterA(config)# access-list 15 deny host 192.168.144.2

Extended access lists can filter traffic based on Layer 4 protocols and both source and destination IP addresses, but standard access lists cannot. The range used for extended access lists is 100 to 199 and 2000 to 2699 (expanded range). The expanded range is an additional set of numbers that can also be used for extended access lists.

Access lists cannot filter traffic that has originated from the filtering router. For this reason, an access list cannot filter packets based on a router's IP address.

In review:

- Standard access list can filter based on source IP address
- Extended access lists can filter traffic based on Layer 4 protocols and by both source and destination IP addresses

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces

References:

https://www.cisco.com/c/en/us/td/docs/ios/sec_data_plane/configuration/guide/12_4/sec_data_plane_12_4_book/sec_access_list_ov.html
https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

QUESTION 42
What is the default administrative distance of a static route?

A. 90
B. 0
C. 1
D. 110

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

While the administrative distance of a route can be altered, there are default administrative distance values assigned to various methods of learning routes. When a static route is defined, it will have an administrative distance of 1.

An administrative distance value of 90 is the default assigned to EIGRP.

An administrative distance value of 0 is the default assigned to directly connected routes.

An administrative distance value of 110 is the default assigned to OSPF.

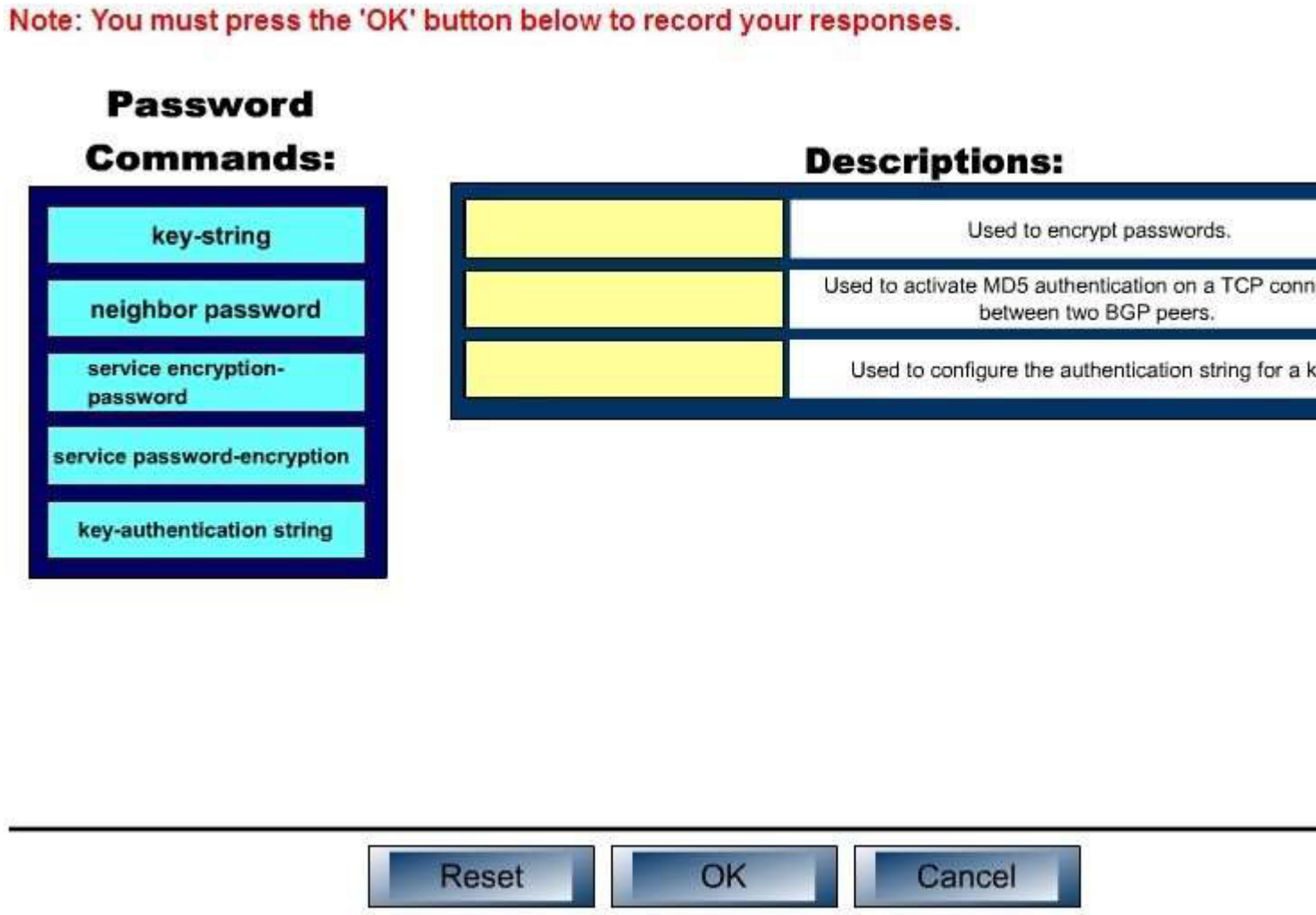
Objective:
Routing Fundamentals

Sub-Objective:
Describe how a routing table is populated by different routing information sources

References:
https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

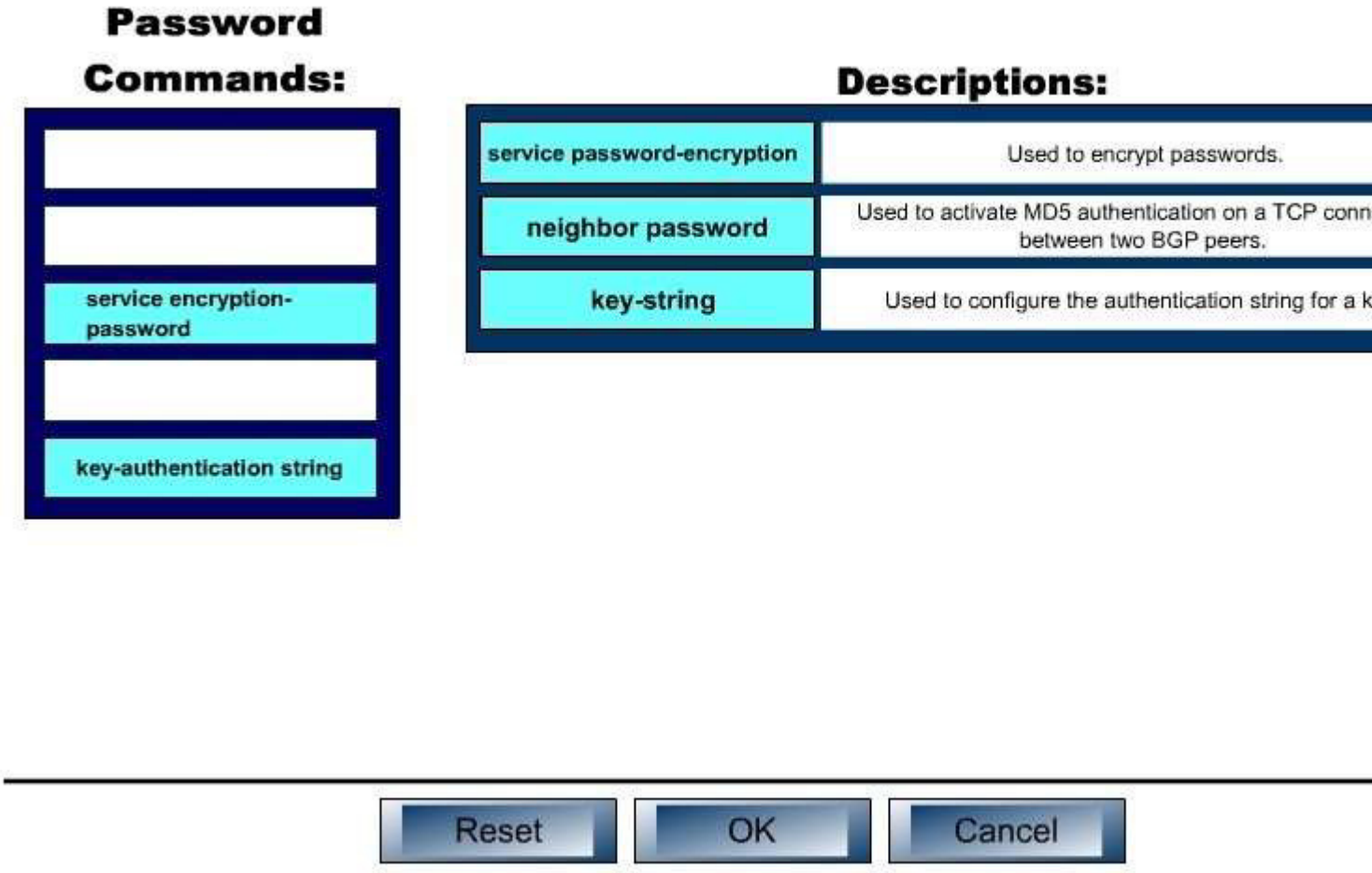
QUESTION 43
DRAG DROP
Click and drag the command(s) used to configure passwords on a Cisco router to their appropriate descriptions. (Not all options will be used.)

Select and Place:



Correct Answer:

Note: You must press the 'OK' button below to record your responses.



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Following are the commands along with their descriptions:

key-string : This command is used to configure the authentication string for a key.

neighbor password : The neighbor password command is used to activate MD5 authentication on a TCP connection between two BGP peers. The complete syntax of this command is: neighbor { ip-address | peer-group-name } password string

service password-encryption : This command is used to encrypt passwords .When executed it will encrypt all text clear text passwords when they are created.

The other options offered are not valid commands.

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure, verify, and troubleshoot basic devicehardening

References:

https://www.cisco.com/c/en/us/support/index.html

https://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book/irg_bgp3.html#wp1097736

QUESTION 44
A router is running several routing protocols, and as a result has learned three routes to the 192.168.5.0 network. Below are the details about the three learned routes:

Routing Protocol Cost
RIP 5
OSPF 25
EIGRP 2269571

Based on this information, which route will be placed in the routing table?

A. the RIP route
B. the OSPF route
C. the EIGRP route
D. all of the routes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The EIGRP route will be placed in the routing table. When a router learns multiple routes to a network from different routing table population methods, which includes routes from routing protocols and static routes created by the administrator, it does so in two steps:

1. It selects the route with the lowest administrative distance.
2. If multiple routes exist with equal administrative distance (usually meaning they learned from the same routing protocol), it chooses from the routes by selecting the one with the lowest cost.

Since EIGRP has the lowest default administrative distance (90), the EIGRP route will be chosen.

The RIP route will not be chosen because it has a default administrative distance of 120.

The OSPF route will not be chosen because it has a default administrative distance of 110.

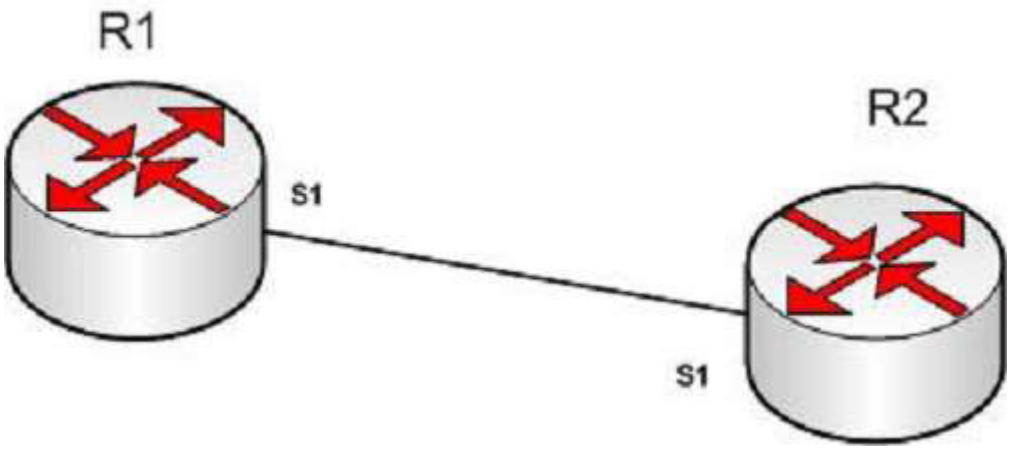
Objective:
Routing Fundamentals

Sub-Objective:
Describe how a routing table is populated by different routing information sources

References:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

QUESTION 45
R1 and R2 are connected as shown in the diagram and are configured as shown in output in the partial output of the show run command.



R1#show run

version 12.0
hostname R1

interface s1
ip address 192.168.5.5 255.255.255.252

ip host R1 192.168.5.6

R2#show run

version 12.0
hostname R2
interface s1
ip address 192.168.5.6 255.255.255.252
ip host R1 192.168.5.5

The command ping R2 fails when executed from R1. What command(s) would allow R1 to ping R2 by name?

A. R1(config)#int S1R1(config-if)#no ip address 192.168.5.5R1(config-if)# ip address 192.168.5.9 255.255.255.252
B. R1(config)#no ip host R1R1(config)# ip host R2 192.168.5.6 255.255.255.252
C. R1(config)#no hostname R2R1(config)# hostname R1
D. R2(config)#int S1R1(config-if)#no ip address 192.168.5.5R1(config-if)# ip address 192.168.5.9 255.255.255.0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Both routers have been configured with the ip host command. This command creates a name to IP address mapping, thereby enabling the pinging of the device by address. On R1, the mapping is incorrect and needs to

be corrected. Currently it is configured as ip host R1 192.168.5.6. It is currently mapping its own name to the IP address of R2.

To fix the problem, you should remove the incorrect IP address mapping and create the correct mapping for R2, as follows:

R1(config)#no ip host R1
R1(config)# ip host R2 192.168.5.6 255.255.255.252

Once this is done, the ping on R2 will succeed.

The IP address of the S1 interface on R1 does not need to be changed to 192.168.5.9 /30. In fact, if that is done the S1 interface on R1 and the S1 interface in R2 will no longer be in the same network. With a 30-bit mask configured, the network they are currently in extends from 192.168.5.4 - 192.168.5.7. They are currently set to the two usable addresses in that network, 192.168.5.5 and 192.168.5.6.

The hostnames of the two routers do need to be set correctly using the hostname command for the ping to function, but they are correct now and do not need to be changed.

The subnet mask of the S1 interface on R2 does not need to be changed to 255.255.255.0. The mask needs to match that of R1, which is 255.255.255.252.

Objective:
Infrastructure Services

Sub-Objective:
Troubleshoot client connectivity issues involving DNS

References:

https://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

QUESTION 46
Which two modes are Cisco Internetwork Operating System (IOS) operating modes? (Choose two.)

A. User Privileged mode
B. User EXEC mode
C. Local configurationmode
D. Global configuration mode
E. NVRAM monitor mode

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

User EXEC mode and global configuration mode are the Cisco IOS operating modes. The following list shows the Cisco IOS operating modes along with their description:

- User EXEC mode: The commands in this mode are used to enable connections to remote devices and change the terminal settings for a short duration. User EXEC commands also enable you to perform basic tests and view system information.
- Global configuration mode: The commands in this mode enable you to make changes to the entire system.
- Privileged EXEC mode: The commands in this mode are used to configure operating parameters. This mode also provides access to the remaining command modes.
- Interface configuration mode: The commands in this mode allow you to change the operation for interfaces such as serial or Ethernet ports.

- ROM monitor: The commands in this mode are used to perform low-level diagnostics.

All the other options are incorrect because they are not valid Cisco IOS operating modes.

To enter privileged EXEC mode, you must enter the command enable on the router. You will then be prompted for the enable password, if one has been created.

To enter global configuration mode, you must first enterprivileged EXEC mode (see above) and then enter the command configure terminal (which can be abbreviated to config t), and the router will enter a mode that allows you to make global configuration changes.

Objective:
Network Fundamentals

Sub-Objective:
Select the appropriate cabling type based on implementation requirements

References:

https://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/mgx_8850/software/mgx_r3/rpm/rpm_r1-1/configuration/guide/appc.html#wp1002608

QUESTION 47
Based on the command output below, which of the interfaces on Router1 are trunk ports?

```
Router1# show mac-address-table

Dynamic Addresses Count: 14
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count: 23
Total MAC addresses: 33
Non-static Address Table:
Destination Address Address Type VLAN Destination Port

------------------- ------------ ---- --------------------

0010.0de0.e289 Dynamic 1 FastEthernet0/1
0010.7b00.1540 Dynamic 1 FastEthernet0/5
0010.7b00.1545 Dynamic 1 FastEthernet0/5
0060.5cf4.0076 Dynamic 3 FastEthernet0/1
0060.5cf4.0077 Dynamic 3 FastEthernet0/1
0060.5cf4.1315 Dynamic 2 FastEthernet0/1
0060.70cb.f301 Dynamic 1 FastEthernet0/2
00e0.1e42.9978 Dynamic 1 FastEthernet0/3

<output omitted>
```

A. Fa0/1
B. Fa0/2
C. Fa0/3
D. Fa0/5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Interface Fa0/1 is a trunk port. The output shows that it has MAC addresses that belong to VLANs 1, 2 and 3. Only trunk ports can carry traffic from multiple VLANs.

Fa0/2 is not a trunk port. It only carries traffic from VLAN 1.

Fa0/3 is not a trunk port. It only carries traffic from VLAN 1.

Fa0/5 is not a trunk port. It only carries traffic from VLAN 1.

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:
https://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

QUESTION 48
Which Cisco Internetwork Operating System (IOS) command is used to assign a router a name for identification?

A. description
B. banner motd
C. hostname
D. banner exec

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The hostname command is used to assign the router a name for identification. This command is a global configuration mode command. The syntax of the command is as follows:

Router(config)# hostname [name]

The name parameter of the command specifies the new host name for the router.

The description command is incorrect because this command is used to set a description for an interface. The description command is an interface configuration mode command.

The banner motd command is used to specify a message of the day (MOTD) banner to users logging into the router. This is a global configuration mode command, but it does not assign a name to the router for identification.

The banner exec command enables a banner message to be displayed when an EXEC process is created; for example, if a line is activated or an incoming connection is made to a telnet line.

Objective:
Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_f1.html#wp1015617

QUESTION 49
Which of the following IPV6 commands is used to define a static host name-to-address mapping in the host name cache?

A. ipv6 host
B. ipv6 unicast routing
C. ipv6 neighbor
D. ipv6 local

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The ipv6 host command is used to define a static host name-to-address mapping in the host name cache, and is executed in global configuration mode.

The ipv6 unicast-routing command is used to enable IPv6 forwarding on a router.

There is no ipv6 local command. There is an ipv6 local pool command that can be used to define a prefix pool when using DHCPv6.

The ipv6 neighbor command is used to configure a static entry in the IPv6 neighbor discovery cache, which will enhance the neighbor discovery process that occurs with IPv6.

Objective:
Infrastructure Services

Sub-Objective:
Troubleshoot client connectivity issues involving DNS

References:

https://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_06.html#wp2170954

QUESTION 50
Which of the following commands would allow you to determine the bandwidth of an interface?

A. show interfaces
B. show interfaces accounting
C. show cdp
D. show cdp neighbors

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show interfaces command shows information about each interface including a section on the bandwidth of the connection. If you wanted to locate this information in the output, it would be in the third down line as follows:

MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255,load 1/255

Where BW = bandwidth

The show interfaces accounting command focuses on the relative amounts of traffic going through each interface, but does not indicate the bandwidth.

The show cdp command shows information about the Cisco Discovery protocol, a Layer 2 protocol used by Cisco devices to advertise their existence and capabilities to other Cisco devices ion the network.

The show cdp neighbors command shows information about each discovered neighbor, but does not display the bandwidth of an interface.

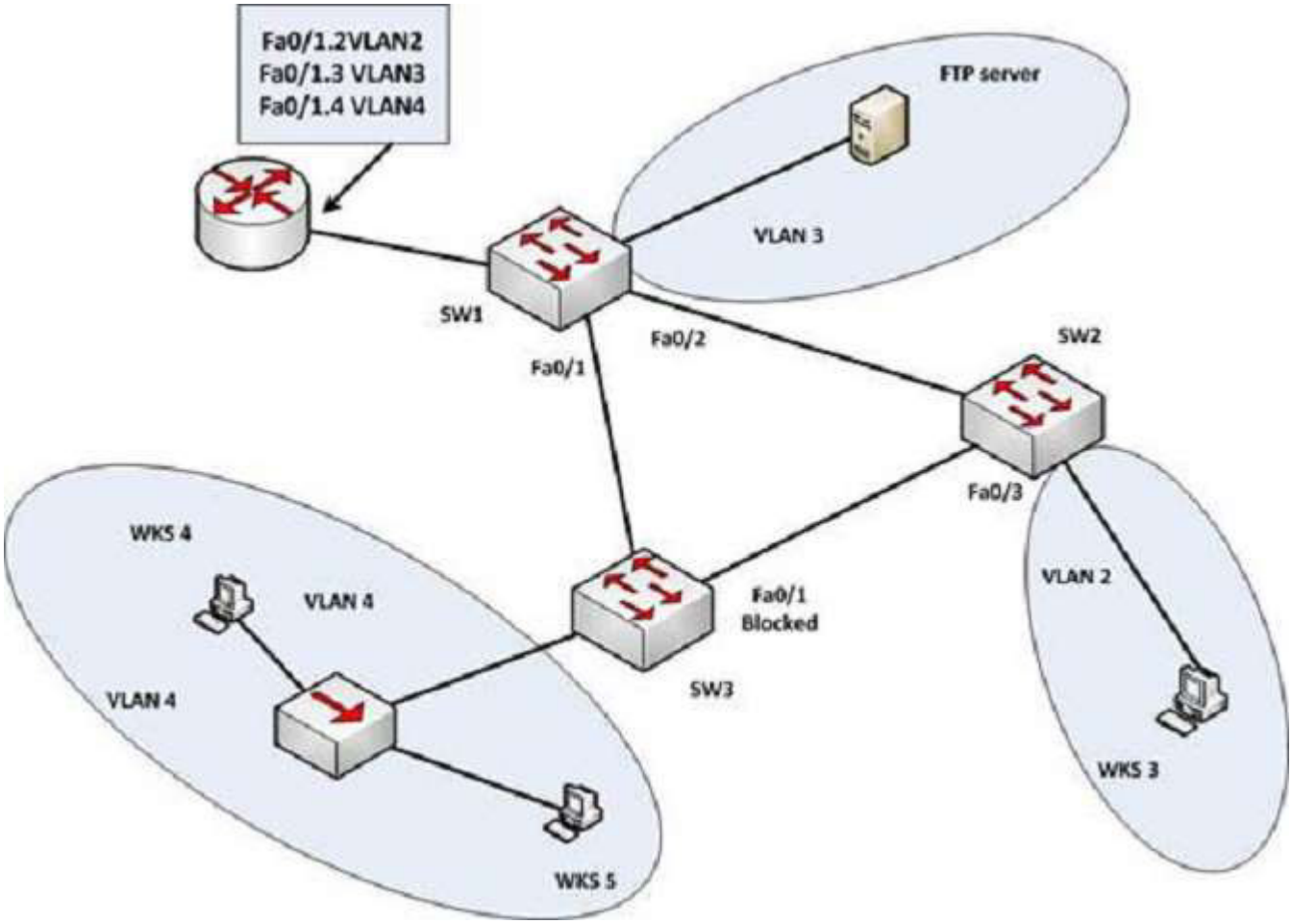
Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

https://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

QUESTION 51
What statements are NOT true regarding the network shown below?



A. If Fa0/1.4 goes down WKS4 will not be able to contact the FTP server
B. Collisions can occur between WKS4 and WKS5
C. STP is running
D. SW1 is the root bridge
E. WKS 5 and WKS 3 are in the same network

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

WKS 5 and WKS 3 are NOT in the same network. WKS 5 is in VLAN 4 and WKS 3 is in VLAN 2. VLANs are configured as different subnets serviced by sub interfaces on the router. Each of the sub interfaces is a different subnet or different network.

It is true that if Fa0/1.4 goes down, WKS4 will not be able to contact the FTP server. WKS3 and the FTP server are in different VLANs, which means that if either of the subinterfaces on the router servicing VLAN 3 or VLAN 4 go down, they not be able to connect, since all inter-VLAN communication goes through the router using those subinterfaces. Since Fa0/1.4 services VLAN 4, where WKS4 is located if Fa0/1.4 goes down WKS4 will not be able to contact the FTP server.

It is true that collisions can occur between WKS4 and WKS5 since they are in the same VLAN and connected

to a hub. If they were connected to a switch, collisions would NOT be possible.

It is true that STP is running. It runs on the switches by default.

It is true that SW1 is the root bridge.Since the Fa0/1 port on SW3 is in a blocking state and STP rules call for forwarding on all ports that lead to the root bridge, then SW2 cannot be the root bridge. Since all ports must be forwarding on the root bridge, that rules out SW3 as the root bridge, which mean SW1 must be the root bridge.

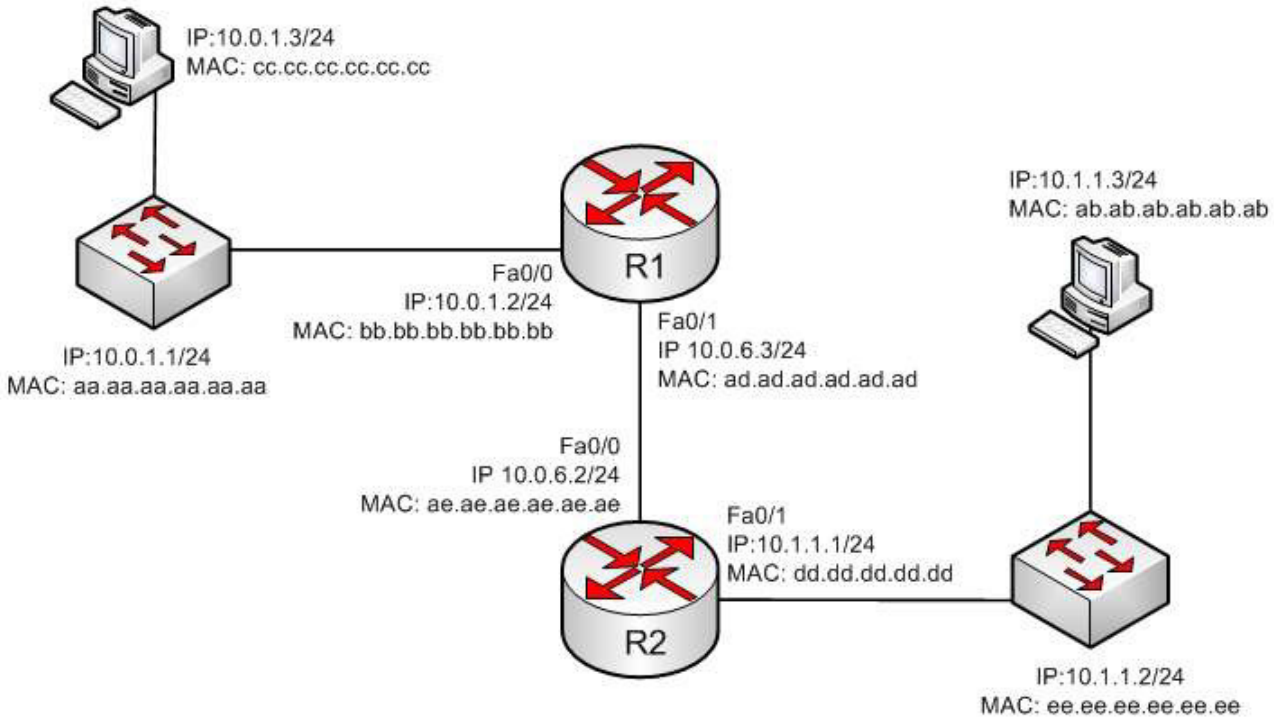
Objective:
Routing Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot inter-VLAN routing

References:

http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_LAN_Switching#LAN_Switching

QUESTION 52
In the diagram below, when a packet sent from the PC at 10.0.1.3 to the PC at 10.1.1.3 leaves the Fa0/1 interface of R1, what will be the source and destination IP and MAC addresses?



A. source IP 10.1.1.2 destination IP 10.1.1.3Source MAC ad.ad.ad.ad.ad.ad destination MAC ab.ab.ab.ab.ab.ab
B. source IP 10.1.1.1 destination IP 10.1.1.3Source MAC ad.dd.dd.dd.dd.dd.dd destination MACab.ab.ab.ab.ab.ab
C. source IP 10.0.1.3 destination IP 10.1.1.3Source MAC ad.ad.ad.ad.ad.ad destination MAC ae.ae.ae.ae.ae.ae
D. source IP 10.0.6.3 destination IP 10.1.1.3Source MAC ad.ad.ad.ad.ad.ad destination MAC ae.ae.ae.ae.ae.ae

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

The source IP address will be 10.0.1.3 and the destination IP address will be 10.1.1.3. The source MAC address will be ad.ad.ad.ad.ad.ad and the destination MAC address will be ae.ae.ae.ae.ae.ae.

The source and destination IP addresses never change as the packet is routed across the network. The MAC address will change each time a router sends the packet to the next router or to the ultimate destination. The switches do not change either set of addresses in the header; they just switch the frame to the correct switch port according to the MAC address table. Therefore, when the packet leaves R1, the source MAC address will be that of R1 and the destination MAC address will be that of the Fa0/0 interface of R2. The IP addresses will be those of the two workstations, 10.0.1.3 and 10.1.1.3.

When the workstation at 10.0.1.3 starts the process, it will first determine that the destination address is in another subnet and will send to its default gateway (10.0.1.2). It will perform an ARP broadcast for the MAC address that goes with 10.0.1.2, and R1 will respond with its MAC address, bb.bb.bb.bb.bb.bb.

After R2 determines the next-hop address to send to 10.0.1.3 by parsing the routing table, it will send the packet to R1 at 10.0.6.2. When R2 receives the packet, R2 will determine that the network 10.0.1.0/24 is directly connected and will perform an ARP broadcast for the MAC address that goes with 10.0.1.3. The workstation at 10.0.1.3 will respond with its MAC address, ab.ab.ab.ab.ab.ab.

Objective:
Routing Fundamentals

Sub-Objective:
Describe the routing concepts

References:

http://docwiki.cisco.com/wiki/Routing_Basics

QUESTION 53
The following shows the partial output of the show cdp neighbors command:

DevicID Local Intrfce Holdtme Capability Platform Port ID
lab-7206 Eth 0 157 R 7206VXR Fas 0/0/0
lab-as5300-1 Eth 0 163 R AS5300 Fas 0
lab-as5300-2 Eth 0 159 R AS5300 Eth 0
lab-as5300-3 Eth 0 122 R AS5300 Eth 0
lab-as5300-4 Eth 0 132 R AS5300 Fas 0/0
lab-3621 Eth 0 140 R S 3631-telcoFas 0/0
008024 2758E0 Eth 0 132 T CAT3000 1/2
lab-400-1 Eth 0 130 r FH400 Fas 0/0

What does "r" represent in this output?

A. Router
B. Route bridge
C. Hub
D. Repeater

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The "r" in the output of the show cdp neighbors command is a capability code that represents a repeater. The capability codes from the output of the show cdp neighbors command along with their descriptions are:

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

The show cdp neighbors command is used to view details about neighboring devices discovered by Cisco Discovery Protocol (CDP). The following code is the full output of the command:

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
DevicID Local Intrfce Holdtme Capability Platform Port ID
lab-7206 Eth 0 157 R 7206VXR Fas 0/0/0
lab-as5300-1 Eth 0 163 R AS5300 Fas 0
lab-as5300-2 Eth 0 159 R AS5300 Eth 0
lab-as5300-3 Eth 0 122 R AS5300 Eth 0
lab-as5300-4 Eth 0 132 R AS5300 Fas 0/0
lab-3621 Eth 0 140 R S 3631-telcoFas0/0
008024 2758E0 Eth 0 132 T CAT3000 1/2
lab-400-1 Eth 0 130 r FH400 Fas 0/0

The fields in the output are as follows:

Device ID: The ID, Media Access Control (MAC) address or the serial number of the neighboring device.
Local Interfce: The protocol which the connectivity media uses.
Holdtime: The time duration for which the CDP advertisement will be held back by the current device from a transmitting router before it gets discarded.
Capability: The type of device discovered by the CDP. It can have the following values:

- R Router
- T Transparent bridge
- B Source-routing bridge
- S Switch
- H Host
- I IGMP device
- r Repeater

Platform: The product number of the device.
Port ID: The protocol and port number of the device.

The "r" in the output does not represent a router. A router would be represented by a capital "R."

The "r" in the output does not represent a route bridge. A source route bridge would be represented by a capital "B."

The "r" in the output does not represent a hub. The show cdp neighbors command does not include a capability code for this device.

Objective:
LAN Switching Fundamentals

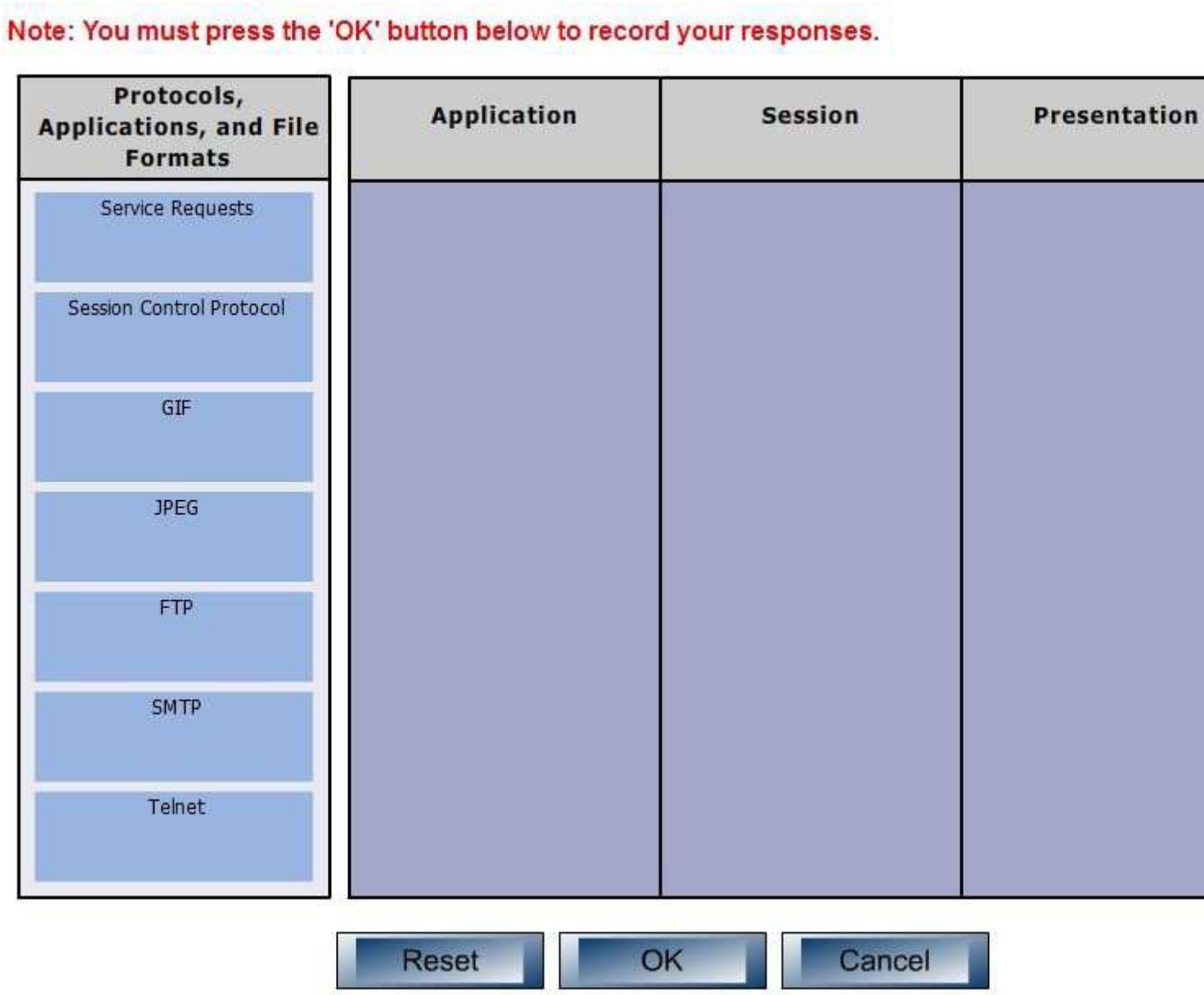
Sub-Objective:
Configure and verify Layer 2 protocols

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html#wp1074517

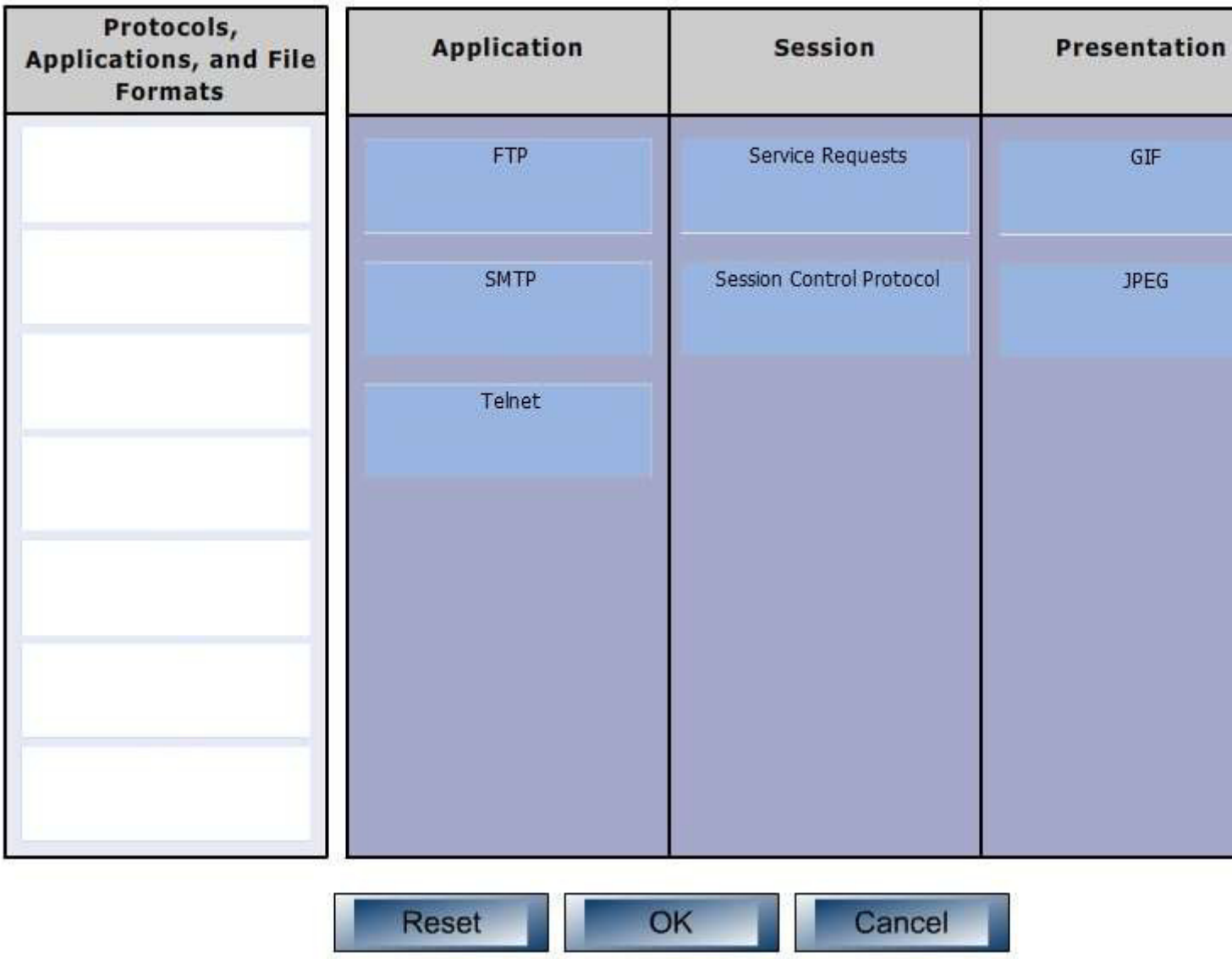
QUESTION 54
DRAG DROP
Click and drag the following protocols, applications, and file formats on the left, to their corresponding Open Systems Interconnection (OSI) layers.

Select and Place:



Correct Answer:

Note: You must press the 'OK' button below to record your responses.



Section: (none)
Explanation

Explanation/Reference:
Explanation:

The application layer is responsible for interacting directly with the application. It provides application services such as e-mail and File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and telnet. Some of its associated protocols include:

- FTP: Used to transfer data between hosts through the Internet or a network.
- SMTP: SMTP is a Transmission Control Protocol (TCP)/Internet Protocol (IP) protocol which is used to send and receive e-mail messages.
- Telnet: Used to allow remote logins.

The session layer is used to create, manage, and terminate sessions between communicating nodes. Some of the protocols and applications associated with this layer include:

- Service requests: Service requests and service responses which take place between different applications are handled by the session layer.
- Session Control Protocol (SCP): Allows a host to have multiple conversations with another host using the same TCP connection.

The Presentation layer in the OSI model enables coding and conversion functions for application layer data. The formatting and encryption of data is done at this layer, as the Presentation layer converts data into a format which is acceptable by the application layer. Some of the file types associated with this layer include:

- Graphics Interchange Format (GIF)
- Joint Photographic Experts Group(JPEG)
- Tagged Image File Format (TIFF)

Other layers in the OSI model include:

- Transport: Responsible for error free and sequential delivery of data. This layer is used to manage data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Physical: Consists of hardware for sending and receiving data on a carrier. The protocols which work at the Physical layer include Fast Ethernet, RS232,and Asynchronous Transfer Mode (ATM).
- Network: Used to define the network address or the Internet Protocol (IP) address which is then used by the routers to forward make forwarding decisions.
- Data Link: Ensures reliable transmission of data across a network on the basis of Layer 2 addresses such as MAC addresses (Ethernet) or DLCIs (Frame Relay).

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast TCP and UDP protocols

References:

http://docwiki.cisco.com/wiki/Internetworking_Basics#OSI_Model_and_Communication_Between_Systems

QUESTION 55
Which of the following loop avoidance mechanisms drives the requirement to create subinterfaces for each point-to-point connection in a partially meshed frame relay network?

A. split horizon
B. poison reverse
C. maximum hop count
D. feasible successor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Split horizon is the loop avoidance mechanism that drives the requirement to create sub interfaces for each point-to-point connection in a partially meshed frame relay network. Frame relay is a non-broadcast multi-access (NBMA) network and obeys the rules of split horizon. This mechanism prohibits a routing protocol from sending updates out the same physical interface on which it was received. When the same physical interface is

used to host multiple frame relay connections, this will prevent an update arriving from remote network A on the physical interface from being sent out the same interface to remote network B.

By creating a subinterface for each frame relay connection and assigning IP addresses to the subinterfaces rather than the physical interface, and by placing the subinterfaces into different subnets, split horizon will not see the "virtual" interfaces as the same interface and will allow these routing updates to be sent back out the same physical interface on which they arrived. It is important to map each subnet (or subinterface) to a remoteData Link Connection Identifier (DLCI) so that traffic to a remote network can be sent out the correct subinterface.

To summarize this discussion:

- Subinterfaces solve the NBMA split horizon issues.
- There should be one IP subnet mapped to each DLCI

Poison reverse is not the mechanism driving the requirement to create subinterfaces for each point-to-point connection in a partially meshed frame relay network. This mechanism requires a router to send an unreachable metric to the interface on which a network was discovered when it is learned from another interface that the network is no longer available.

Maximum hop count is not the mechanism driving the requirement to create sub interfaces for each point-to-point connection in a partially meshed frame relay network. Each routing protocol has a maximum hop count, which is the maximum number of hops allowed to a remote network before the network is considered "unreachable".

Feasible successor is not the mechanism driving the requirement to create sub interfaces for each point-to-point connection in a partially meshed frame relay network. This is a concept unique to EIGRP that represents a secondary route to a network that is considered the "best" route of possible backup routes.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure and verify Layer 2 protocols

References:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html#splithorizon

QUESTION 56
You are a network administrator, and you are configuring an access list to permit Hypertext Transfer Protocol (HTTP) traffic based on the source and destination IP address of the devices.

What access list (ACL), protocol, and port number will you configure to permit HTTP traffic? (Choose three.)

A. 23
B. 80
C. TCP
D. UDP
E. Standard
F. Extended

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:

Explanation:

An extendedACL can filter network traffic on the basis of source and destination IP address, the transport layer protocol (such as TCP or UDP), and the port number. HTTP, or general Web traffic, uses TCP at the Transport layer and port 80. More port numbers commonly used in ACLs include:

- HTTPS 443
- FTP 20, 21
- Telnet 23
- DNS 53
- SMTP 25

Standard ACLs can filter only on the source IP address inside a packet, whereas an extended ACL can filter on the source and destination IP addresses in the packet, the IP protocol, and protocol information such as the destination port number. An extended ACL therefore allows you to filter more precisely. For example, you can filter a specific Telnet session from one of your users' PCs to a remote Telnet server. Standard ACLs do not support this form of granularity. With a standard ACL, you can either permit or deny all traffic from a specific source device.

Port 23 is incorrect because this port is used by Telnet. Therefore, port 23 does not need to be configured to permit HTTP traffic.

UDP is incorrect because HTTP uses TCP.

Standard ACLs cannot filter traffic based on the destination IP addresses. Therefore, this option is incorrect.

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces

References:

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

https://www.cisco.com/c/en/us/td/docs/ios/sec_data_plane/configuration/guide/12_4/sec_data_plane_12_4_book/sec_access_list_ov.html

QUESTION 57
A newly implemented IP-based video conferencing application is causing the network to slow down. Which OSI layer needs to be addressed to resolve the problem?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4
E. Layer 5
F. Layer 6
G. Layer 7

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You need to address Open System Interconnect (OSI) Layer 1, the Physical layer, to resolve the problem. IP-based video conferencing applications are bandwidth-intensive and may cause the network to slow down unless there is enough bandwidth to ensure proper network operation. To resolve bandwidth problems, you may need to switch to a higher capacity network backbone, whichmay require a change of cabling or media types, such as fiber optics. Cabling and network media types are defined at OSI Layer 1.

The seven layers of the OSI model are as follows, in descending order from Layer 7 to Layer 1:

- Application: Interacts directly with the application. It provides application services, such as e-mail and File Transfer Protocol (FTP).
- Presentation: Enables coding and conversion functions for application layer data. The Presentation layer converts data into a format that is acceptable by the application layer. The formatting and encryption of data is done at this layer.
- Session: Creates, manages, and terminates sessions between communicating nodes. The session layer handles the service requests and responses that take place between different hosts.
- Transport: Delivers data sequentially and without errors. This layer manages data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Network: Defines the network address or the Internet Protocol (IP) address, which is then used by the routers to forward the packets.
- Data Link: Ensures the reliable delivery of data to the physical address of the destination.
- Physical: Describes the physical medium used to convert the data to bits. Examples include fiber optic, wireless, and Ethernet.

Objective:
Network Fundamentals

Sub-Objective:
Apply troubleshooting methodologies to resolve problems

References:

http://docwiki.cisco.com/wiki/Internetworking_Basics#OSI_Model_and_Communication_Between_Systems

QUESTION 58
You are attempting to add an IP address to an interface on a router with which you are unfamiliar. You type the following command and receive the following error:

```
Router78(config)#interfce Serial0
^
%invalid input detected at '^' marker.
```

Which of the following could be a reason for receiving this message?

A. the command syntax is incorrect
B. the interface type does not exist on this router
C. the command is entered at the wrong prompt
D. the interface is configured already

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command has a syntax error. The word interface is misspelled as indicated by the marker.

The interface type may not exist on the router, but that is not the problem with this specific error message. If

you attempt to access an interface that is not present on the router, it will elicit this same message, but the marker will be placed at the beginning of the interface type as shown below. The interface information is in lines 14-19.

Router78(config)#interface Serial0
^
%invalid input detected at '^' marker.

When you are unfamiliar with a router, it is best to execute the show version command, which will indicate the type and number of interfaces on the router as shown below:

```
Router78# show version
Cisco IOS Software, 3800 Software (C3845-IPBASE-M), Version 12.3(11)T7, RELEASE SOFTWARE (f
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sat 30-Jul-05 03:12 by dchih

ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)

Router78 uptime is 10 weeks, 6 days, 9 hours, 30 minutes
System returned to ROM by power-on
System restarted at 05:09:07 CDT Thu Oct 20 2005
System image file is "flash:c3845-ipbase-mz.123-11.T7.bin"

Cisco 3845 (revision 1.0) with 419839K/104448K bytes of memory.
Processor board ID FTX0938A5PE
2 Gigabit Ethernet interfaces
27 Serial interfaces
1 ISDN Basic Rate interface
6 terminal lines
2 Channelized T1/PRI ports
1 Subrate T3/E3 port
DRAM configuration is 64 bits wide with parity enabled.
479K bytes of NVRAM.
62720K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102
```

The command is not entered at the wrong prompt. It should be entered at the global configuration prompt.

If the interface were already configured, it would still allow you to access the interface and make changes.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.4>Interface Configuration Overview

QUESTION 59
Which cable can suffer attenuation if it is bent beyond the minimum bend radius?

A. UTP
B. STP
C. Co-axial
D. Fiber optic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Fiber-optic cables can suffer attenuation if they are bent beyond the minimum bend radius. Fiber-optic cables work on the principle of total internal reflection. The fiber optic cable uses a laser and glass tubes with refractive internalcoating to achieve total internal reflection. If a light ray travelling in the tube is bent at a certain angle, the light ray will be reflected inside the medium instead of passing through the medium. If the fiber optic cables are bent beyond the minimum bend radius, the signal will be lost and the cable will suffer attenuation. Fiber cables are expensive and are typically used for outdoor campus backbone. However, as the fiber cables use light to carry signals, they are not affected by the electro-magneticinterference (EMI) generated by electric cables.

Another advantage of fiber optic cabling is its applicability to situations where electrical issues may exist in the environment. Even in situations where the length of the cable run is well within the attenuation limits of STP (for example 55 meters), voltage differences between buildings can cause issues. That is a problem that can be solved by using fiber on the run, which is not impacted by electrical issue.

All other cables typically use copper to carry low voltage signals and are not affected by normal bending. However, even copper cables may suffer some signal loss if there are bends in the cable.

Objective:
Network Fundamentals

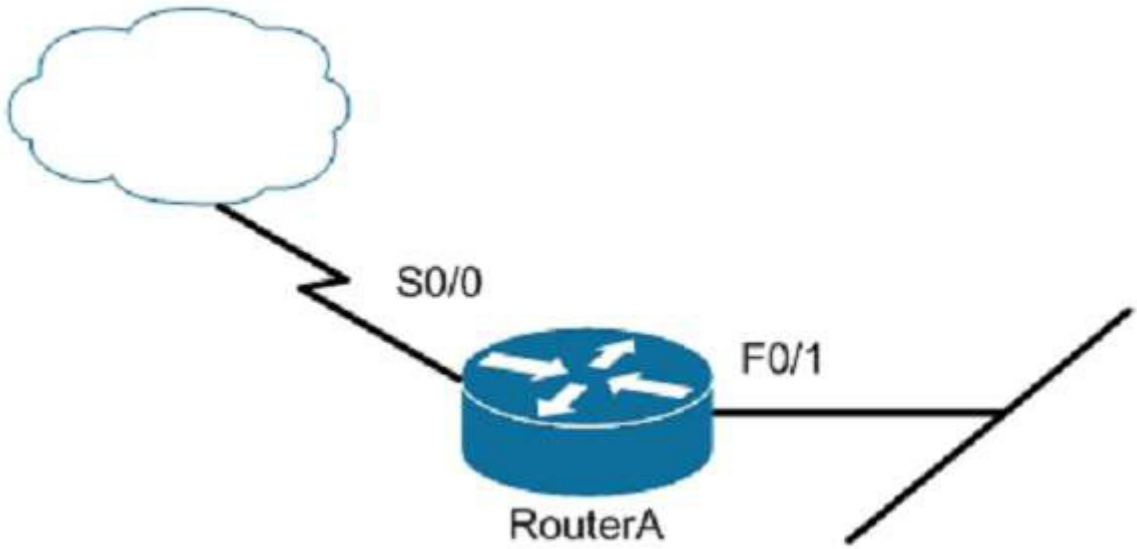
Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

http://www.ciscopress.com/articles/article.asp?p=170740&seqNum=10

QUESTION 60
Users on the LAN are unable to access the Internet. How would you correct the immediate problem?



Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol
FastEthernet 0/0 unassigned YES unset down down
FastEthernet 0/1 172.16.1.254 YES NVRAM up up
Serial0/0 200.16.4.25 YES NVRAM administratively down down
Serial0/1 unassigned YES unset down down

A. Configure a bandwidth on the serial interface.
B. Perform a no shutdown command on the serial interface.
C. Configure a private IP address on the Fastethernet0/0 LAN interface.
D. Change the IP address on the serial interface.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The output indicates that the serial interface leading to the Internet is administratively down. All router interfaces are disabled by default due to the presence of a shutdowncommand in the running configuration. The no shutdown command removes this configuration, and the interface becomes active. The command sequence is:

Router(config)# interface serial0/0
Router(config-if)# no shutdown

Although it was not the problem in the scenario, the S0/0 interface could also cause an error if it is configured as shown in this output:

Interface IP-Address OK? Method Status Protocol

Serial0/0 200.16.4.25 YES NVRAM up down

In this example, the S0/0 interface has been enabled, and while there is Layer 1 connectivity (the Status column), Layer 2 is not functioning (the Protocol column). There are two possible reasons for this result:

- Interface S0/0 is not receiving a clock signal from the CSU/DSU (if one is present).
- The encapsulationtype configured on S0/0 does not match the type configured on the other end of the link (if the other end is a router).

Configuring a bandwidth on the serial interface is incorrect because the output indicates the interface is administratively down,which does not pertain to bandwidth.

Configuring a private IP address on the Fastethernet0/0 LAN interface is incorrect because the output indicates the problem is with the disabled serial interface.

The IP address on the serial interface may or may no tbe valid, but it is not the immediate cause of the connectivity problem. The serial interface is disabled.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

https://www.cisco.com/c/en/us/td/docs/server_nw_virtual/2-5_release/command_reference/admin.html#wp1045355

QUESTION 61
Which of the following statements is NOT true regarding flow control?

A. It determines the rate at which the data is transmitted between the sender and receiver.
B. It can help avoid network congestion.
C. It manages the data transmission between devices.
D. It uses a cyclic redundancy check (CRC) to identify and remove corrupted data.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

It is NOT true that flow control uses a cyclic redundancy check (CRC) to identify and remove corrupted data. CRC is an error-checking schema that checks and removes corrupted data. It is a calculation that is performed at the source. Flow control uses CRC to identify corrupted data for the purpose of requesting re-transmission, but it does not use CRC to remove the corrupted data from the packet. If corruption is detected, the entire packet will be dropped.

Flow control is a function that ensures that a sending device does not overwhelm a receiving device. The following statements are TRUE regarding flow control:

- Flow control controls the amount of data that the sender can send to the receiver.
- Flow control determines the rate at which the data is transmitted between the sender and receiver.
- Flow control of certain types can aid in routing data around network congestion

Types of flow control include windowing, buffering, and congestion avoidance:

- Windowing- a process whereby the sender and receiver agree to increase or decrease the number of packets

received before an acknowledgment is required based on network conditions. This packet number is called a window. When conditions are favorable, the window size will be increased. During unfavorable network conditions, it will be decreased.
- Buffering- the ability of a network card to store data received but not yet processed in a buffer (memory). This enhances its ability to handle spikes in traffic without dropping any data.
- Congestion avoidance - a process that some routing protocols can perform by adding information in each frame that indicates the existence of congestion on the network, allowing the router to choose a different routing path based on this information.

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast OSI and TCP/IP models

References:

http://docwiki.cisco.com/wiki/Internet_Protocols#TCP_Packet_Format

QUESTION 62
Which of the following statements are TRUE regarding the following output? (Choose all that apply.)

```
Router# show ip route

Gateway of last resort is 192.168.15.1 to network 0.0.0.0

<<output omitted>>
D 192.168.10.0 [90/2172416] via 192.168.15.254, 0:01:42, Serial0/1/0
C 192.168.14.0 is directly connected, Serial0/0/0
D 192.168.52.0 [90/2172416] via 192.168.15.254, 0:00:35, Serial0/1/0
[90/2172416] via 192.168.15.5, 0:02:05, Serial0/0/0
C 192.168.15.0 is directly connected, Serial0/1/0
C 192.168.20.0 is directly connected, Serial0/0/1
S 192.168.50.0 [1/0] via 192.168.53.1
C 192.168.33.0 is directly connected, Loopback1
D 192.168.25.0 [90/2196545] via 192.168.20.254, 0:01:20, Serial0/0/1
```

A. There are four default routes on this router.
B. There are four physically connected interfaces on this router.
C. This router is running EIGRP.
D. The metric for the routes learned via a routing protocol is 90.
E. A packet for the 192.168.52.0 network will be load-balanced across two paths.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

This router is running EIGRP and a packet for the 192.168.52.0 network will be load-balanced across two paths.

EIGRP routes display with a D code in the leftmost column of the show ip route command. The D stands for Diffusing Update Algorithm (DUAL), which is the algorithm used by EIGRP to determine the best and potential backup paths to each remote network. There are four EIGRP-learned routes in this exhibit.

When two routes with equal metrics exist in the routing table, EIGRP will send packets using both paths. In the output there are two routes listed for the 192.168.52.0 network. Both have thesame metric value (2172416). Therefore, packets will be sent to that network via the Serial 0/1/0 interface to the neighbor at 192.168.15.254 and via the Serial 0/0/0 interface to the neighbor at 192.168.15.5. Both paths, either directly or indirectly, lead to the 192.168.52.0 network, and both paths have the same cost.

There are not four default routes on this router. The D represents EIGRP-learned routes, not default routes. There is one default route, as indicated by the line of output that says Gatewayof last resort is 192.168.15.1 to network 0.0.0.0. Because Serial0/1/0 is directly connected to the 192.168.15.0 network, packets that are destined for networks not found in the routing table will be sent out on that interface.

The C in the leftmost column of the show ip route command represents directly connected networks, of which there are four in the exhibit. Closer examination, however, reveals that one of these entries (for network 192.168.33.0) is connected to a loopback interface (Loopback1), as opposed to a physical interface:

C 192.168.33.0 is directly connected, Loopback1

Loopback interfaces are virtual, software interfaces that appear in the routing table, but do not represent a physical interface on the router. Therefore, there are three physically connected interfaces on this router, not four.

The metric for the routes learned via a routing protocol is not 90. The 90 in the scenario output is the administrative distance (AD) of the route, and the 2196545 is the metric value (see below):

D 192.168.25.0 [90/2196545] via 192.168.20.254, 0:01:20, Serial0/0/1

Objective:
Routing Fundamentals

Sub-Objective:
Interpret the components of routing table

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book.html

QUESTION 63
You are configuring all your devices for IPv6. Which of the following is the only device that requires the ipv6 unicast-routing command?

A. Layer 2 switch
B. Router
C. Adaptive security appliance
D. Wireless AP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Only the router requires the ipv6 unicast-routing command. The command ipv6 unicast-routing enables the routing of IPv6 packets on a router. It is not required when you are simply configuring interfaces on devices that participate in IPv6.

A Layer 2 switch can have an IPv6 address applied to its management interface and to any VLAN interfaces. However, because the switch does no routing, it does not require the ipv6 unicast-routing command.

An adaptive security appliance (ASA) can also have IPv6 addresses applied to its interfaces and can route both IPv6 and IPv4 traffic. However, it does not require the ipv6 unicast-routing command.

A wireless access point differs from a wireless router in that it operates as a switch or hub and does no routing. Therefore, it does not require this command.

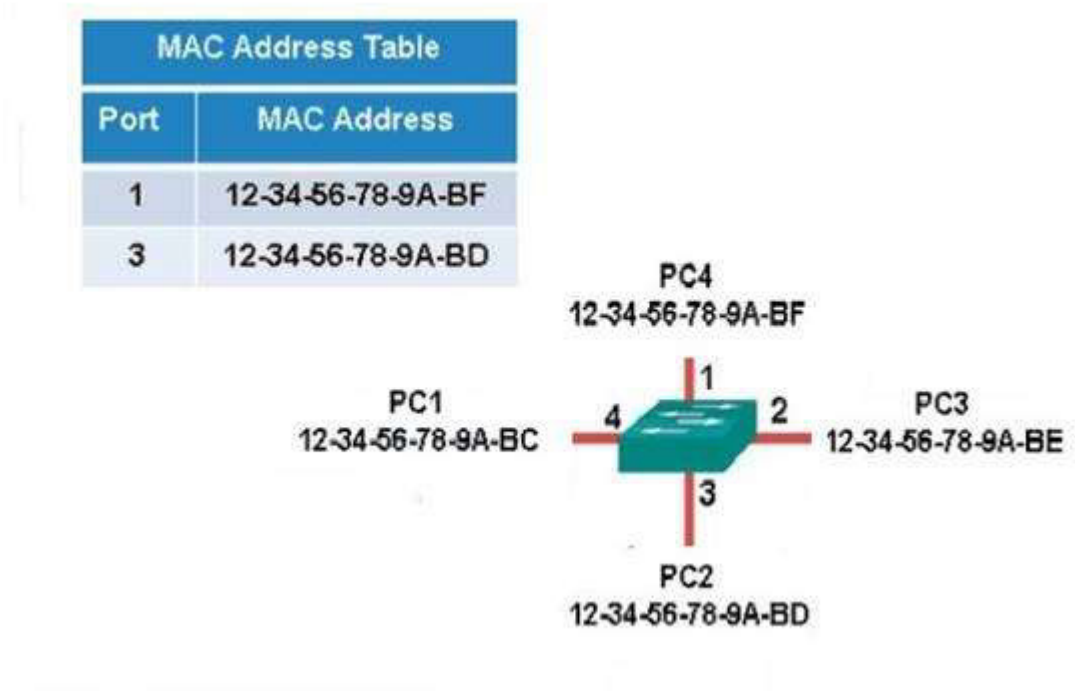
Objective:
Network Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot IPv6 addressing

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-15-2s-book.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book/ipv6-i5.html#wp2095571844

QUESTION 64
The following exhibit displays the MAC address table of a switch in your network, along with the location of each device connected to the switch:



Which of the following frames will be flooded to all ports after it is received by the switch?

A. source MAC: 12-34-56-78-9A-BD, destination MAC: 12-34-56-78-9A-BF
B. source MAC: 12-34-56-78-9A-BF, destination MAC:12-34-56-78-9A-BD
C. source MAC: 12-34-56-78-9A-BF, destination MAC: 12-34-56-78-9A-BC
D. source MAC: 12-34-56-78-9A-BC, destination MAC: 12-34-56-78-9A-BF

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

The frame with a source MAC of 12-34-56-78-9A-BF and a destination MAC of12-34-56-78-9A-BC would be sent to all ports because the destination MAC address is not already in the MAC address table.

The frame with a source MAC of 12-34-56-78-9A-BD and a destination MAC of 12-34-56-78-9A-BF would not be sent to all ports because the destination MAC address is in the MAC address table.

The frame with a source MAC of 12-34-56-78-9A-BF and a destination MAC of 12-34-56-78-9A-BD would not be sent to all ports because the destination MAC address is in the MAC address table.

The framewith a source MAC of 12-34-56-78-9A-BC and a destination MAC of 12-34-56-78-9A-BF would not be sent to all ports because the destination MAC address is in the MAC address table.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Interpret Ethernet frame format

References:

http://www.ciscopress.com/articles/article.asp?p=2339639&seqNum=2

https://www.globalknowledge.com.eg/about-us/Knowledge-Center/Article/How-do-Switches-Work/

QUESTION 65
What data structure is pictured in the graphic?

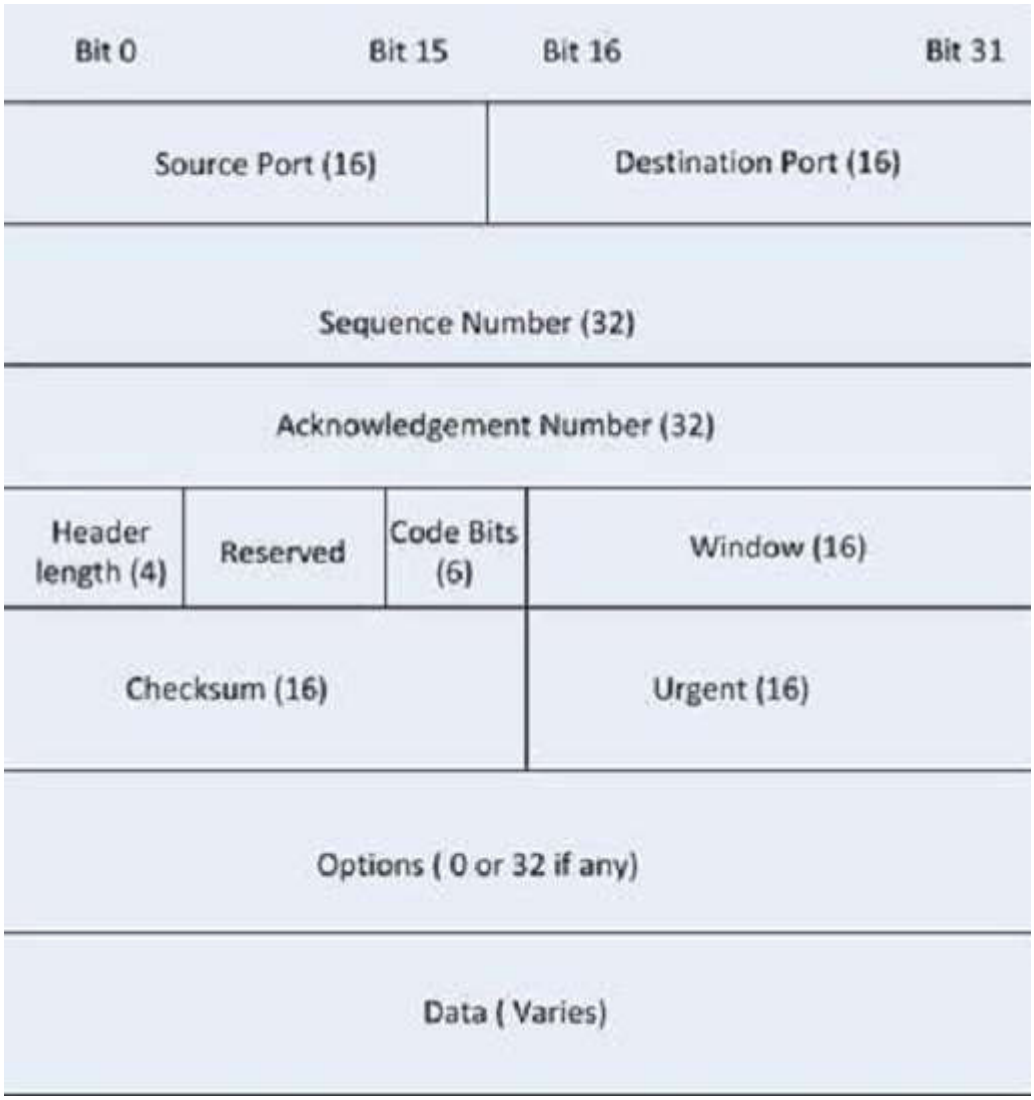
A. TCP segment
B. UDP datagram
C. IP header
D. Http header

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The data structure pictured in the graphic is an UDP datagram. It uses a header (not shown) that contains the source and destination MAC address. It has very little overhead as compared to the TCP segmented (shown later in this explanation) as any transmission that uses UDP is not provided the services of TCP.

It is not a TCP segment, which has much more overhead (shown below). The TCP header contains fields for sequence number, acknowledgment number, and windows size, fields not found in a UDP header because UDP provides none of the services that require use of these fields. That is, UDP cannot re-sequence packets that arrive out of order, nor does UDP acknowledge receipt (thus the term non-guaranteed to describe UDP). Furthermore, since UDP does not acknowledge packets there is no need to manage the window size (the window size refers to the number of packets that can be received without an acknowledgment.



It is not an IP header. An IP header contains fields for the source and destination IP address. The IP header, like the UDP segment, does not contain fields for sequence number, acknowledgment number, and windows size, fields not found in a TCP header because TCP provides none of the services that require use of these fields. IP provides best-effort user data. This does not cause a delivery problem, however, as IP relies on TCP to provide those services when the transmission is a unicast.

An HTTP header does not include fields for HTTP requests and responses.

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast TCP and UDP protocols

References:

http://docwiki.cisco.com/wiki/Internet_Protocols

QUESTION 66
Your assistant just entered the following command on a router:

R67(config)#logging trap 0

Which of the following levels will be trapped? (Choose all that apply.)

A. Emergency
B. Alert
C. Critical
D. Error
E. Warning
F. Notification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When the logging trap command is used and a level number is specified, then only that level and any levels with a LOWER level number will be trapped. The levels numbers and their names are shown below:

- Emergency(severity 0) - The system is unusable
- Alert (severity 1) - Immediate action is needed
- Critical (severity 2) - Critical condition
- Error (severity 3) - Error condition
- Warning (severity 4) - Warning condition
- Notification (severity 5) - Normal but significant condition
- Informational (severity 6) - Informational message
- Debugging (severity 7) - Debugging message

Since level 0 was specified, then only Level 0 messages (Emergency) will be trapped.

None of the other levels will be trapped because they all have level values over 0, which was specified in the logging trap command.

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure and verify device-monitoring using syslog

References:

http://www.ciscopress.com/articles/article.asp?p=101658&seqNum=3

QUESTION 67
Which Cisco IOS command is used to view the information about the interfaces on which Cisco Discovery

Protocol (CDP) is enabled?

A. show cdp interface
B. show interfaces
C. show cdp
D. show cdp interfaces

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show cdp interface command is used to view the information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled.

The syntax of the command is as follows:

Router# show cdp interface [type number]

The parameters of the command are as follows:

type: specifies the type of interface for which information is required
number: specifies the number of interfaces for which information is required

The output of the show cdp interface command is as follows:

Router#show cdp interface
Serial0 is up, line protocol is up, encapsulation is SMDS
Sending CDP packets every 100 seconds
Holdtime is 300 seconds
Serial1 is up, line protocol is up, encapsulation is SMDS
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
Sending CDP packets every 120 seconds
Holdtime is 360 seconds

The show interfaces command is incorrect because this command is used to view configured interfaces on the router. The output of this command can be very useful, especially when troubleshooting a connection with no connectivity. Consider the output of the command on the following two routers that are connected with a serial interface:

NewYork#show interfaces s0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet Address is 192.168.10.1/24
MTU 1500 bytes,BW 1544 Kbit
Reliability 255/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)

LosAngeles#show interfaces s1
Serial0 is up, line protocol is up
Hardware is HD64570
Internet Address is 192.168.11.2/24
MTU 1500 bytes,BW 56000 Kbit
Reliability 255/255

Encapsulation HDLC, loopback not set
Keepalive set (10 sec)

Notice that the following settings are correct:

- The encapsulation matches (HDLC)
- The physical connection is good (indicated by Serial0 is up)

Notice, however, that the IP addresses 192.168.10.1 and 192.168.11.2 are NOT in the same subnet when using a 24-bit mask. With a 24-bit mask, the two addresses should agree through the first three octets, and these do not. Problems such as this can be located through inspection of the output produced by the show interfaces command.

The show cdp command is incorrect because this command is used to view the global CDP information.

The show cdp interfaces command is incorrect because this command does not exist in the Cisco command reference. There is a show cdp interface command, which displays CDP activity on a per-interface basis.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure and verify Layer 2 protocols

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html#wp1013043

QUESTION 68
Which switch port will be in a blocking state? (Click the Exhibit(s) button to view the switch port diagram.)

A. SwitchA Fa0/1
B. SwitchA Fa0/2
C. SwitchB Fa0/1
D. SwitchB Fa0/2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

SwitchB will be forwarding on F0/1, and blocking on F0/2.

SwitchA will become the STP root bridge due to its lower MAC address. All ports on the root bridge will become designated ports in a forwarding state. SwitchB has redundant connectivity to the root bridge, and must block one of its interfaces to prevent a switching loop. STP will use its operations to determine which of the redundant interfaces on SwitchB to block to prevent a switchingloop

Both interfaces are the same speed (FastEthernet), and thus their cost to the root is the same.

Finally, the interface with the lowest number will become the forwarding port. F0/1 has a lower port number than F0/2, so F0/1 becomes a forwarding port, and F0/2 becomes a blocking port.

Note: Unlike STP, Rapid Spanning Tree Protocol (RSTP) uses the term "discarding" for a switch port that is not forwarding frames.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html

QUESTION 69
In which two situations would it be appropriate to issue the ipconfig command with the /release and /renew options? (Choose two.)

A. When the result of running the ipconfig /all command indicates a 169.254.163.6 address
B. When recent scope changes have been made on the DHCP server
C. When no IP helper address has been configured on the router between the client and the DHCP server
D. When the no ip directed-broadcast command has been issued in the router interface local to the client, and no IP helper address has been configured on the router between the client and the DHCP server

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

It would it be appropriate to issue the ipconfig command with the /release and /renew options when the result of running the ipconfig /all command indicates a 169.254.163.6 address, or when recent scope changes have been made on the DHCP server. When a computer has an address in the 169.254.0.0 network, it indicates that the computer has not been issued an address from the DHCP server. Instead, the computer has utilized Automatic Private IP Addressing (APIPA) to issue itself an address. If the reason for this assignment is a temporary problem with the DHCP server or some other transitory network problem, issuing the ipconfig / release command followed by the ipconfig /renew command could allow the computer to receive the address from the DHCP sever.

Similarly, if changes have been made to the settings on the DHCP server, such as a change in the scope options (such as gateway or DNS server), issuing this pair of commands would update the DHCP client with the new settings when his address is renewed.

These commands will have no effect when no IP helper address has been configured on the router between the client and the DHCP server. An IP helper address can be configured on the local interface of a router when no DHCP server exists on that subnet and you would like to allow the router to forward DHCP DISCOVER packets to the DHCP server on a remote subnet. DHCP DISCOVER packets are broadcast, and routers do not

pass on broadcast traffic by default.

These commands also will be of no benefit if the no ip directed-broadcast command has been issued in the router interface local to the client and no IP helper address has been configured on the router between the client and the DHCP server. The no ip directed-broadcast command instructs the router to deny broadcast traffic (which is the default). Under those conditions, the command will not result in finding the DHCP server or receiving an address.

Objective:
Infrastructure Services

Sub-Objective:
Troubleshoot client- and router-based DHCP connectivity issues

References:
https://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

QUESTION 70
During the process of connecting four switches to the central router and implementing VLANS between the devices, it becomes apparent that there was a misunderstanding about which encapsulation protocol to use on the links between the switches and the router.

If there is mismatch between the encapsulation types used on the router interface and the type used on the connected switch port, what will be the result?

A. The relevant switch ports will be green.
B. The relevant switch ports will be amber.
C. The relevant switch ports will be neither green nor amber.
D. The relevant switch ports will be green and flashing.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

If there is a mismatch between the encapsulation types used on the router interface and the type used on the connected switch port, the link will not be functional and there will be neither an amber nor a green light. The same outcome will be produced when there is a bad cable, an incorrect cable type, or a lack of signal. An example of a cable mismatch would be the use of a straight-through cable when the situation required a crossover cable, or vice versa.

When connecting switch ports to routers, there are two possible encapsulation types: the default Interswitch Link (ISL) and the 802.1q standard. ISL is a Cisco proprietary technology; therefore, it can only be used between Cisco products. 802.1q is an industry standard that can be used between Cisco and non-Cisco products. If the same type is not configured on each end, the link will not work.

The relevant switch ports will not be green. Green indicates normal operation with no activity.

The relevant switch ports will not be amber. Amber indicates the link is administratively down. The amber light is usually flashing as well.

The relevant switch ports will not be green and flashing. This display indicates normal operation with activity on the line.

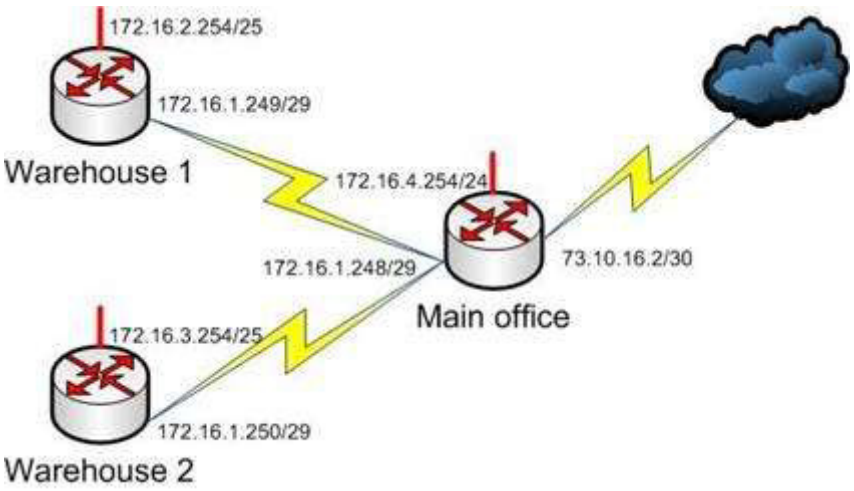
Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

https://www.cisco.com/c/en/us/products/hw/tsd_products_support_end-of-sale_and_end-of-life_products_list.html

QUESTION 71
The router interfaces for a network are configured as shown in the following exhibit. (Click the Exhibit(s) button.)



Warehouse 1 is having trouble connecting to the Internet. After troubleshooting the issue, several other connectivity issues are discovered.

What should you do to fix this problem?

A. Change the IP address of the Warehouse 1 LAN interface.
B. Change the IP address of the Warehouse 1 WAN interface.
C. Change the IP address of the Main Office LAN Interface.
D. Change the IP address of the Main Office WAN interface.
E. Change the IP address of the Main Office Internet interface.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You should change the IP address of the Main Office WAN interface.

With a 29-bit mask and the chosen class B address,the following network IDs are created:

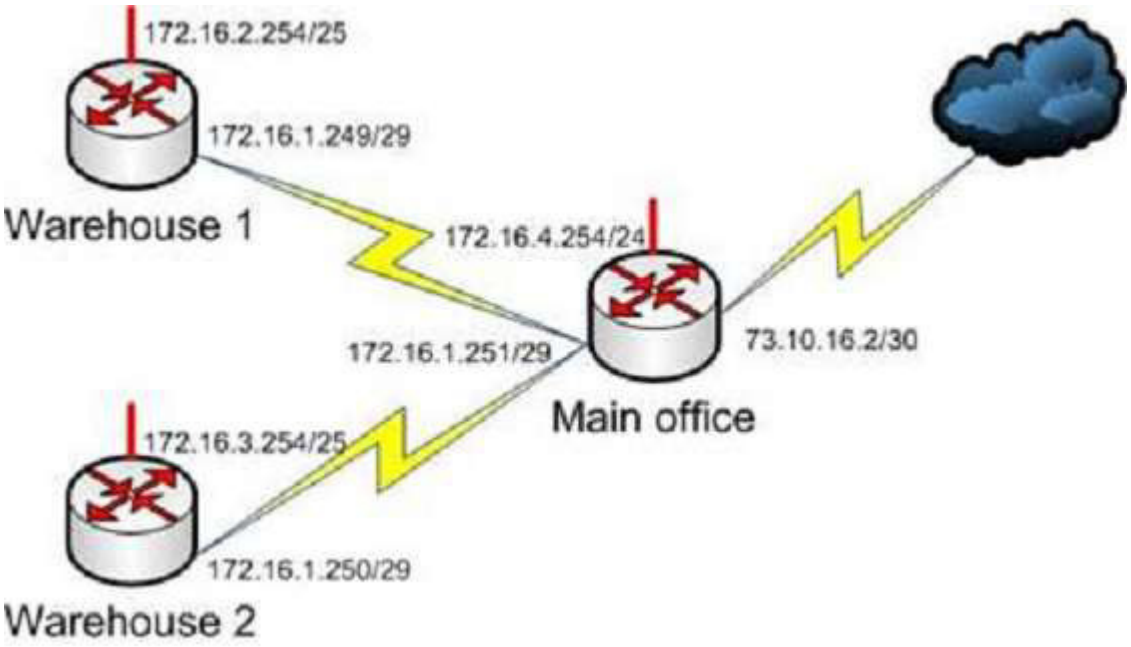
172.16.0.0
172.16.0.8
172.16.0.16
172.16.0.24
172.16.0.32
172.16.0.40

172.16.0.48
172.16.0.56
172.16.0.64
and so on, incrementing each time by 8 in the last octet. At the end of this series of increments, the network IDs will be:

172.16.1.240
172.16.1.248
172.16.2.0

172.16.1.248/29 is the subnet number for the WAN. This address cannot be used as a host address on the network. The legitimate addresses in this range are 172.16.0.249 through 172.16.0.254. This misconfiguration would cause both the Warehouse 1 and Warehouse 2 segment to have trouble connecting to the Internet.

All of the other addresses in the diagram are correct. The correct configuration of the network is shown in the following diagram:



Objective:
Network Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

QUESTION 72
Which of the following is NOT a VLAN Trunking Protocol (VTP) mode of operation?

A. client
B. server
C. virtual
D. transparent

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Virtual is not a valid VTP mode of operation. There are three different VTP modes of operation: client, server, and transparent.

In client mode, a switch can synchronize VLAN information with the domain and forward advertisements. However, VLANs cannot be created, deleted, or modified from a switch in client mode. Also, a client mode switch does not save VLAN information in non-volatile Random Access Memory (NVRAM). It is stored in Flash in a file called vlan.dat.

In server mode, a switch synchronizes the VLAN information with the domain, sends and forwards advertisements, and can create, delete, or modify VLANs. In server mode, VLAN information is stored in Flash in a file called vlan.dat.

In transparent mode, a switch does not synchronize its VLAN configuration with the domain, but it forwards advertisements. VLANs can be created, deleted, or modified locally and VLAN configuration is saved in both the running-config file in RAM and in flash in a file called vlan.dat.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot VLANs (normal range) spanning multiple switches

References:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25sg/configuration/guide/conf/vlans.html

QUESTION 73
Which command would be used to establish static translation between an inside local address 192.168.144.25 and an inside global address 202.56.63.102?

A. router(config)#ip nat inside source static 192.168.144.25 202.56.63.102
B. router(config)#ip source natinside static local-ip 192.168.144.25 global-ip 202.56.63.102
C. router(config)#ip nat static inside source 192.168.144.25 202.56.63.102
D. router(config)#ip nat inside static source 192.168.144.25 202.56.63.102

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To establish a static translation between an inside local address 192.168.144.25 and an inside global address 202.56.63.102, you would use the ip nat inside source static 192.168.144.25 202.56.63.102 command executed in global configuration mode. The correct format of the command is:

ip nat inside source static local-ip global-ip

This static configuration can be removed by entering the global no ip nat inside source static command.

Simply executing the ip nat inside source command will not result in NAT functioning. The NAT process also has to be applied correctly to the inside and outside interfaces. For example if, in this scenario the Fa0/0 interface hosted the LAN and the S0/0 interface connected to the Internet the following commands would

complete the configuration of static NAT.

```
Router(config)#interface F0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface S0/0
Router(config-if)#ip nat outside
```

The other options are incorrect because they are not valid Cisco IOS configuration commands. They all contain syntax errors.

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot inside source NAT

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book.html

https://www.cisco.com/c/en/us/tech/ip/ip-addressing-services/tech-tech-notes-list.html

QUESTION 74
Which of the following values will be used by a router to make a routing decision when two routes have been learned from OSPF?

A. cost
B. administrative distance
C. composite metric
D. hop count

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When two routes have been learned by OSPF to same network, the best route will be chosen based on lowest cost. Cost is the metric used in OSPF to choose the best route from all candidate routes learned through OSPF.

Administrative distance is a measure of the trustworthiness of the routing information source. It is a value used by a router to choose between multiple known routes that have been learned from different routing sources, such as different routing protocols. When routes are learned from the same routing protocol, their administrative distance will be equal, and the router will then choose the route with the lowest metric value of the routing protocol. In this case, that metric is the OSPF cost.

The composite metric is the metric used by EIGRP to choose a route when multiple routes have been learned by EIGRP.

Hop count is the metric used by RIP to choose a route when multiple routes have been learned by RIP.

Objective:
Routing Fundamentals

Sub-Objective:
Describe how a routing table is populated by different routing information sources

References:

https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8651-21.html

QUESTION 75
Which Cisco IOS command can be used to troubleshoot switch startup problems on a Cisco Catalyst 2950 switch?

A. show test
B. show diagnostic
C. show post
D. show switchstartup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The Cisco IOS command show post is used on the 2900/3500XL, 2950/2955, 3550, 2970, and 3750 series switches to view and troubleshoot issues related to the Power On Self Test (POST) on the switch. This command will find the POST test that failed on startup.

The show test command is incorrect because it is a CatOS command, not a Cisco IOS command. The Cisco 2950 uses a Cisco IOS operating system and not the Catalyst operating system. The show test command is used on a switch to view any hardware errors that occurred at startup. It also provides information on the errors returned from the diagnostic tests. The following parameters can be used with this command:

- mod: An optional parameter used to specify the module number.
- diaglevel: Used to view the diagnostic level.
- diagfail-action: Used to view information on the action taken by the supervisor engine after the failure of a diagnostics test.

The following code is a sample output of this command for module 2:

```
Module 2 : 2-port 1000BaseX Supervisor
Network Management Processor (NMP) Status: (. = Pass, F = Fail, U = Unknown)
ROM: . Flash-EEPROM: . Ser-EEPROM: . NVRAM: . EOBC Comm: .
Line Card Firmware Status for Module 2 : PASS
Port Status :
Ports 1 2
---------
. .
Line Card Diag Status for Module 2 (. = Pass, F = Fail, N = N/A)
Module 2
Cafe II Status :
NewLearnTest: .
IndexLearnTest: .
DontForwardTest: .
DontLearnTest: .
ConditionalLearnTest: .
BadBpduTest: .
TrapTest: .
Loopback Status [Reported by Module 2] :
Ports 1 2
-----------
. .
Channel Status :
Ports 1 2
-----------
```

The show diagnostic command is incorrect because this command is used on the Catalyst 6000 series, not the 2950. A variant of the command, show diagnostics, is used for the Catalyst 4000 series. These commands can be used on the relevant switches to view any hardware errors that occurred on startup. This command displays the Power-On Self Test (POST) results.

The show switchstartup command is not a valid Cisco IOS command.

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:
https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/12027-53.html

https://www.cisco.com/c/en/us/products/hw/tsd_products_support_end-of-sale_and_end-of-life_products_list.html

QUESTION 76
At which layer in the Open Systems Interconnection (OSI) model does flow control generally operate?

A. the Network layer
B. the Transport layer
C. the Physical layer
D. the Session layer

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Flow control generally operates at the Transport layer of the OSI model. The Transport layer is responsible for the error-free and sequential delivery of data. This layer is used to manage data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Flow control does not operate at the Network layer in the OSI model. The Network layer defines the network address or the Internet Protocol (IP) address, which is then used by the routers to forward the packets.

Flow control does not operate at the Physical layer in the OSI model. The Physical layer describes the physical medium (i.e. Ethernet, fiber optic, or wireless) used for sending and receiving data on a carrier.

Flow control does not operate at the Session layer in the OSI model. The Session layer provides the mechanism for opening, closing and managing a session between end-user application processes.

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast OSI and TCP/IP models

References:

http://docwiki.cisco.com/wiki/Internet_Protocols#Figure:_Twelve_fields_comprise_a_TCP_packet

QUESTION 77
Which Cisco IOS Cisco Discovery Protocol (CDP) command displays the IP address of the directly connected Cisco devices?

A. show cdp
B. show cdp devices
C. show cdp traffic
D. show cdp neighbors detail

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Explanation:
The show cdp neighbors detail command displays the IP address of the directly connected Cisco devices. CDP is a Layer 2 (Data Link layer) protocol that finds information about neighboring network devices. CDP does not use Network layer protocols to transmit information because it operates at the Data Linklayer. For this reason, IP addresses need not even be configured on the interfaces for CDP to function. The only requirement is that the interfaces be enabled with the no shutdown command. An example of the output of the show cdp neighbors detail command is as follows:

Tecumsah# show cdp neighbors detail

Device ID: Tacoma
Entry address(es):
IP address: 172.19.169.88

Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime: 123 sec
Version:
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
advertisement version: 2
Duplex: half

Device ID: Topeka
Entryaddress(es):
IP address: 172.19.169.100
Platform: cisco AS5300, Capabilities: Router
<<output omitted>>

The show cdp devices command is incorrect because this is not a valid Cisco IOS command.

The show cdp command is incorrect because this command is used to view the global CDP information. It lists the default update and holdtime timers, as in the following sample output:

Atlanta# show cdp
Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2advertisements is enabled

The show cdp traffic command is incorrect because this command displays traffic information between network devices collected by the CDP, as in the following example:

Birmingham# show cdp traffic
Total packets output: 652, Input: 214
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid: 0, Fragmented: 0
CDP version 1 advertisements output: 269, Input: 50
CDP version 2 advertisements output: 360, Input: 25

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html#wp1074517

QUESTION 78
A host is powered up, but the connected switch port does not turn amber or green. Which of the following methods would you use to troubleshoot the situation? (Choose three. Each answer is a complete solution.)

A. Ensure the switch is powered up.
B. Reinstall Windows on the workstation.
C. Reseat the cable.
D. Ensure that the cable is straight-through.
E. Ensure that the cable is crossover.

Correct Answer: ACD
Section: (none)

Explanation

Explanation/Reference:
Explanation:

A black or unlit switch port LED is symptomatic of a Layer 1 problem. The port LED should first turn amber and then turn solid green when a host is powered up. The amount of time it takes to turn solid green will depend on the Spanning Tree Protocol configuration. If the LED is unlit, you should ensure that the switch is powered up and that a straight-through cable is used to connect a switch port to a host, such as a workstation or a printer. If the switch is powered up and a straight-through cable is used, reseat the cable to ensure a firm connection.

Reinstalling Windows on the workstation will not help because this is a Layer 1 problem having to do with the switch having power or the use of proper cabling.

You should not ensure that the cable is crossover, because straight-through (patch) cables are used to connect switch ports to hosts.
Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/hardware/installation/guide/2960_hg/higover.html#wp1021241

QUESTION 79
Refer to the partial output of the show interfaces command:

```
Serial 0 is administratively down, line protocol is down
Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
Internet address is 134.108.28.8, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 4 packets/sec
1127576 packets input, 447251251 bytes, 0 no buffer
Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
5332142 packets output, 496316039 bytes, 0 underruns
0 output errors, 432 collisions, 0 interface resets, 0 restarts
<<output omitted>>
```

What does the Serial 0 is administratively down, line protocol is down line indicate with certainty?

A. There is no problem with the physical connectivity.
B. There is a configuration problem in the local or remote router.
C. There is a problem at the telephone company's end.
D. The shutdown interface command is present in the router configuration.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

The Serial 0 is administratively down, line protocol is down line in the output of the show interfaces command indicates the following:

- The shutdown interface command is present in the router configuration. This indicates that the administrator might have manually shut down the interface by issuing the shutdown command.
- A duplicate Internet Protocol (IP) address might be in use.

This line does not show that there is no problem with the physical connectivity. Since the interface is administratively shut down, there is no way of determining the operational status of the physical layer.

The Serial 0 is administratively down, line protocol is down line does not indicate a configuration problem in the local or remote router. A problem in the configuration of local or remote router would be indicated by the Serial 0 is up, line protocol is down message.

This line does not show that there is a problem at the telephone company's end. Since the interface is administratively shut down, there is no way of determining the operational status of the physical layer or protocol layer on the other end of the line.

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book.html

QUESTION 80
Which Cisco Internetwork Operating System (IOS) command is used to define an access list by name?

A. ip access-list
B. ip access list
C. ip access-group
D. access-list

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The ip access-list command is used to define an access list by name. This command is issued in the global configuration mode. The correct syntax of the command is as follows:

Router(config)# ip access-list {standard | extended} access-list-name

The parameters of the command are as follows:

- standard: Specifies an standard IP access list.
- extended: Specifies an extended IP access list.

- access-list-name: Specifies the name of the access list.

The ip access list command is incorrect because this command does not exist in Cisco IOS terminology. The correct command syntax is ip access-list.

The ip access-group command is incorrect because this command is used to apply an access list to an interface.

The access-list command is incorrect because this command is used to create a numbered access control list entry.

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces

References:

https://www.cisco.com/c/en/us/support/index.html

QUESTION 81
Which two features do Cisco routers offer to mitigate distributed denial-of-service (DDoS) attacks? (Choose two.)

A. Anti-DDoS guard
B. Scatter tracing
C. Access control lists (ACLs)
D. Flow control
E. Rate limiting

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Cisco routers use access control lists (ACLs) and blackholing features to help mitigate distributed denial-of-service (DDoS) attacks. A DoS attack is an attack in which legitimate users are denied access to networks, systems, or resources. One of the most common DoS attacks is the DDoS attack, which is executed by using multiple hosts to flood the network or send requests to a resource. The difference between DoS and DDoS is that in a DoS attack, an attacker uses a single host to send multiple requests, whereas in DDoS attacks, multiple hosts are used to perform the same task.

Cisco routers offer the following features to mitigate DDoS attacks:

- ACLs: Filter unwanted traffic, such as traffic that spoofs company addresses or is aimed at Windows control ports. However, an ACL is not effective when network address translation (NAT) is implemented in the network.
- Rate limiting: Minimizes and controls the rate of bandwidth used by incoming traffic.
- Traffic-flow reporting: Creates a baseline for the network that is compared with the network traffic flow, helping you detect any intrusive network or host activity.
- Apart from these features offered by Cisco routers, the following methods can also be used to mitigate DDoS attacks:
- Using a firewall, you can block or permit traffic entering a network.
- The systems vulnerable to attacks can be shifted to another location or a more secure LAN.
- Intrusion Detection Systems (IDS), such as Network Intrusion Detection Systems (NIDS) and Host Intrusion

Detection Systems (HIDS), can be implemented to detect intrusive network or host activity such as a DoS attack, and raise alerts when any such activity is detected.

Anti-DDoS guard and scatter tracing are incorrect because these features are not offered by Cisco routers to mitigate DDoS attacks.

Flow control is incorrect because flow control is used to prevent the loss of traffic between two devices.

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure, verify, and troubleshoot basic device hardening

References:

https://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.html

QUESTION 82
Which of the following commands will configure a router to use DNS for hostname resolution?

A. ip dns primary
B. ip domain lookup
C. ip dns server
D. ip name-server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The ip domain lookup command configures the device to use DNS for hostname resolution. It must be accompanied by a command that specifies the location of the DNS server, which is done with the ip name-server command.

The ip dns-primary command is used to configure the device as the primary DNS name server for a domain (zone) and as the start of authority (SOA) record source, which designates the start of a zone.

The ip dns server command is used to make the device a DNS server.

Objective:
Infrastructure Services

Sub-Objective:
Describe DNS lookup operation

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/15-mt/dns-15-mt-book/dns-config-dns.html

QUESTION 83
Which type of switching process requires a switch to wait for the entire frame to be received before forwarding it to a destination port?

A. store and forward

B. cut-through
C. fragment free
D. frame-forward

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The store and forward switching process requires a switch to wait until the entire frame is received before forwarding it to a destination port. The store and forward method increases latency as it buffers the entire frame and runs a Frame Check Sequence (FCS) before forwarding it to destination port. However, it ensures error-free frame forwarding because its filters all frame errors.

The cut-through switching process does NOT require a switch to verify the FCS in a frame before forwarding it to the destination port. This type of internal switching method is faster than the store and forward process, but may forward error frames.

The fragment-free switching process only waits to receive the first 64 bytes of the frame before forwarding it the destination port. Fragment-free internal switching assumes that if there is no error in the first 64 bytes of the data, the frame is error free. The assumption is based on the fact that if a frame suffers a collision, it occurs within the first 64 bytes of data. Fragment-free forwarding speed lies between that of store and forward and cut-through.

The term frame-forward is not a valid internal switching process for Cisco switches.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

References:

http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_LAN_Switching#LAN_Switching

QUESTION 84
You are the network administrator for your company. You wanted to connect the host computers to the switches.

Which cable should you use to ensure the connectivity?

A. Straight-through cable
B. Rollover cable
C. Crossover cable
D. Serial cable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A straight-through cable is a normal four-pair cable with the same order of pin configuration on both ends. These are usually used to connect a computer to the switch or hub's Ethernet ports. The following table shows

the pin layout of a straight-through cable:

Pin No.	Pin No.
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

A rollover cable, also known as rolled cable or Cisco console cable, is used to connect a computer terminal to the console port of a router. The cable pin order at one end of the cable is the reverse of the order at another end. Pin 1 is connected to pin 8, pin 2 top in 7, and so on.

A crossover cable is used to connect two similar devices such as a computer to computer or a switch to a switch, and a computer to a router's Ethernet port.

A serial cable is used on a router's wide area network (WAN) interface to connect to the serial ports. Cisco serial cables generally have a male DB-25 connector on one end and a female DB-25 connector on the other.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

https://www.cisco.com/c/en/us/support/docs/routers/7000-series-routers/12223-14.html

QUESTION 85
Which type of IP address is a registered IP address assigned by the Internet Service Provider (ISP), and represents one or more inside local IP addresses externally?

A. Inside local address
B. Outside local address
C. Inside global address
D. Outside global address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

An inside global address is a registered IP address assigned by the ISP that represents internal local IP addresses externally.

An inside local address is an IP address (usually private) assigned to a host on the internal network. The inside local address is usually not assigned by the service provider, nor used to represent one or more inside local IP addresses externally

An outside local address is the IP address of an outside host as it appears to the internal network. It is not used to represent one or more inside local IP addresses externally

An outside global address is the IP address assigned to a host on the external network by the host owner. The address is allocated from a globally routable address space. It is not used to represent one or more inside local IP addresses externally

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot inside source NAT

References:

https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/4606-8.html

http://www.ciscopress.com/articles/article.asp?p=25273

QUESTION 86
Which Cisco Internetwork Operating System (IOS) command is used to apply an access list to an interface?

A. router(config)# ip access-group
B. router(config-if)# ip access-group
C. router(config)# ip access-list
D. router(config-if)# ip access-list

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The router(config-if)#ip access-group command is used to apply an access list to an interface. This command is issued in interface configuration mode. The syntax of the command is as follows:

router(config-if)# ip access-group {access-list-number|access-list-name} {out|in}

The parameters of the command are as follows:

- out|in: Specifies where the access list will be applied on the router. The out value will cause the router to apply the access list to all outgoing packets. The in value will cause the router to apply the access list to all incoming packets.
- access-list-number: Specifies the number of an access list.
- access-list-name: Specifies the name of the access list.

The router(config)# ip access-group command is incorrect because the ip access-group command should be issued in interface configuration mode.

The router(config)# ip access-list command is incorrect because this command is used to define an access list by name.

The router(config-if)# ip access-list command is incorrect because the ip access-groupcommand is issued in global configuration mode, and is used to define an access list by name.

Objective:
Infrastructure Services

Sub-Objective:
Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces

References:

https://www.cisco.com/c/en/us/support/index.html

QUESTION 87
Which feature is NOT provided by flow control?

A. buffering
B. windowing
C. full duplex transmission
D. source-quench messaging

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The full duplex mode of transmission is not provided by flow control. Full duplex transmission is an Ethernet concept where hosts are able to send and receive at the same time. There are no collisions in a full-duplexEthernet network. A dedicated switch port is required for each node in a full-duplex Ethernet network. Both the host's NIC and the switch port must be capable of operating in full-duplex mode. When full duplex is implemented, no collisions will occur on the link between the switch and the device. That will be one error condition that can be removed from consideration when troubleshooting a full duplex link.

Flow control is a function that prevents network congestion. It does so by ensuring that the transmitting device does not flood the receiving device with data. The following statements are true regarding flow control:

- Controls the amount of data which the sender can send to the receiver.
- Uses buffering, transmitting source-quench messages, and windowing to handle network congestion.
- Determines the rate at which the data is transmitted between the sender and receiver.
- Types of flow control include windowing, buffering, and congestion avoidance.

Flow control generally operates at the Transport layer in the OSI model. The Transport layer is responsible for error-free and sequential delivery of data. This layer is used to manage data transmission between devices.

Buffering is a method by which network devices use to save temporary overflows of excess data into the memory. The data is stored in the memory until it is processed.

Source-quench messages are used by the devices that receive the data to avoid buffer overflow.

Windowing is a scheme in which an acknowledgment is required by the source device from the destination after the transmission of a fixed number of packets.

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast OSI and TCP/IP models

References:
http://docwiki.cisco.com/wiki/Internet_Protocols#Figure:_Twelve_fields_comprise_a_TCP_packet

QUESTION 88
In which of the following IPv6 address assignment methods will the interface receive its IPv6 address from a process native to IPv6, and receive additional parameters from DHCP?

A. Stateless DHCPv6
B. Stateful DHCPv6
C. DHCPv6-PD
D. Stateless autoconfiguration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Stateless DHCPv6 uses a combination of processes to assign a configuration to an IPv6 interface. It uses Stateless AddressAutoconfiguration (SAAC), a process native to IPv6, to assign an IPv6 address to the interface. It uses DHCPv6 to assign other parameters, such as the DNS server and NTP server.

In stateful DHCPv6, the interface will receive the IPv6 address and all other parameters from the DHCP server.

In DHCPv6 Prefix Designation (DHCPv6-PD), the device is assigned a set of IPv6 "subnets." This assignment will consist of a set of IPv6 addresses in the same subnet (such as the address 2001:db8::/60) that the device can dynamically allocate to its interfaces.

Objective:
Network Fundamentals

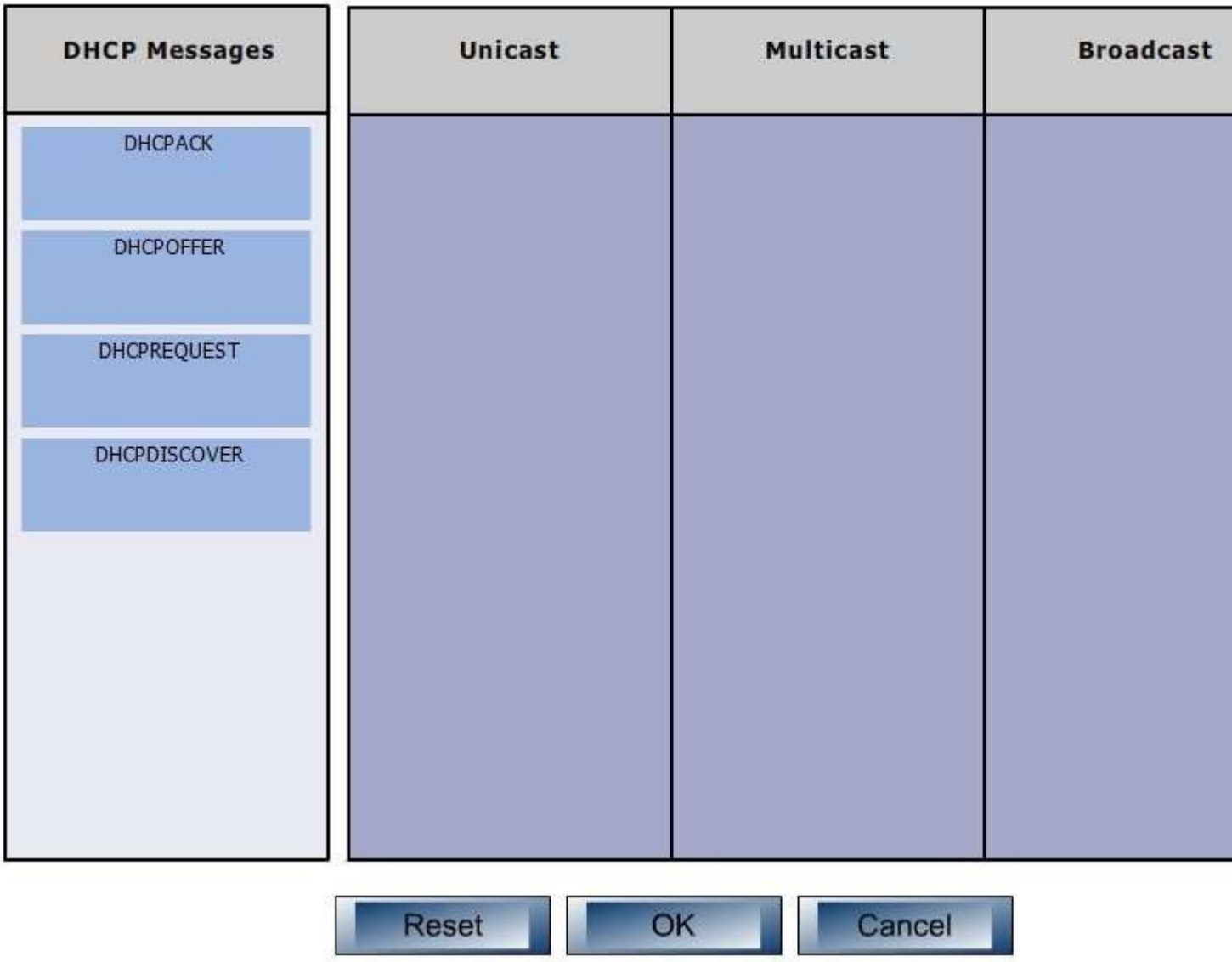
Sub-Objective:
Configure and verify IPv6 Stateless Address Auto Configuration

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book/ip6-dhcp-stateless-xe.html

QUESTION 89
DRAG DROP
Group the special DHCP messages exchanged over the network, on the left, into the different transmission types, on the right.

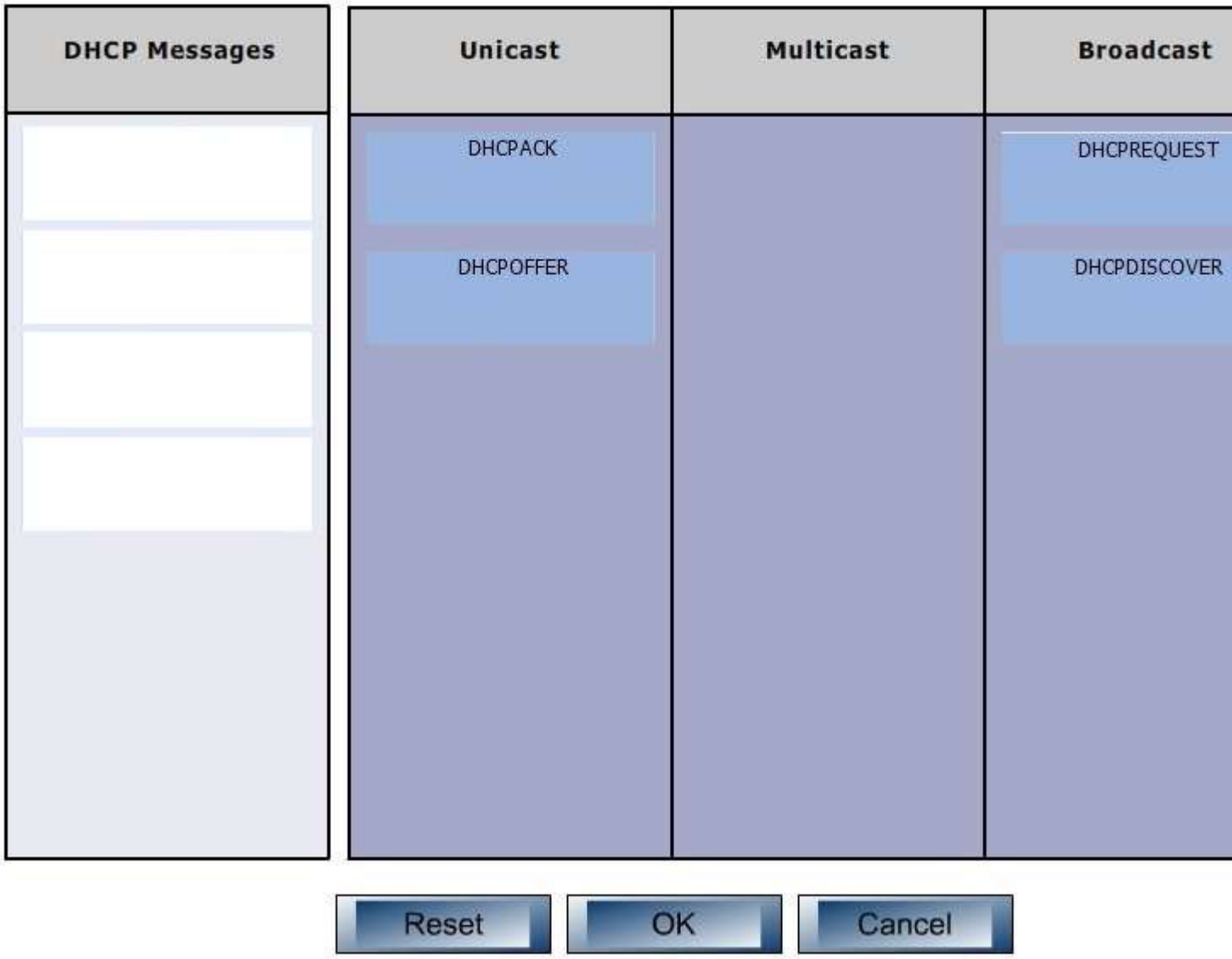
Select and Place:

Note: You must press the 'OK' button below to record your responses.



Correct Answer:

Note: You must press the 'OK' button below to record your responses.



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Dynamic Host Configuration Protocol (DHCP) is an enhancement over Bootstrap Protocol (BOOTP). DHCP is used to automate the distribution of IP address to clients from a central server. BOOTP protocol was also used distribute IP addresses, but was inflexible when changes were made in the network. DHCP offers the following three advantages, which also addressed the inflexibility of the BOOTP protocol:

- Automatic allocation of permanent IP addresses
- Automatic allocation of time bound (leased) IP addresses
- Provision of assigning static IP address or defining a pool of reserved IP address

The following steps are used to allocate IP address dynamically using a CiscoIOS DHCP server:

1. The client device broadcasts a DHCPDISCOVER broadcast message to locate a Cisco IOS DHCP server.
2. The Cisco IOS DHCP server replies with a DHCPOFFER unicast message containing configuration parameters such as an IP address, a MAC address, a domain name, and a lease for the IP address for the client device.
3. The client sends back a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the Cisco IOS DHCP server.
4. The Cisco IOS DHCP server replies to client device with DHCPACK unicast message acknowledging the allocation of the IP address to this client device.

While DHCP is very useful in reducing the administrative burden of issuing IP configurations in a large network, Cisco best practices call for using static IP addressing in a small (6 or fewer hosts) network.

Objective:
Infrastructure Services

Sub-Objective:
Configure and verify DHCP on a router (excluding static reservations)

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html

QUESTION 90
Refer to the following partial output of the show interfaces command:

```
Serial 0 is down, line protocol is down
Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
Internet address is 134.108.28.8, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 4 packets/sec
1127576 packets input, 447251251 bytes, 0 no buffer
Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
5332142 packets output, 496316039 bytes, 0 underruns
0 output errors, 432 collisions, 0 interface resets, 0 restarts
<<output omitted>>
```

What are the two troubleshooting steps that you should perform to resolve the problem depicted in the output? (Choose two.)

A. Check the cable connections.
B. Reset the equipment.
C. Check the router configuration.
D. Check the router configuration for the shutdown interface command.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You should check the cable connections and reset the equipment to troubleshoot the problem depicted in the output. The Serial 0 is down, line protocol is down message indicates that there is no carrier detect (CD) signal sensed by the router. This problem might be due to incorrect cabling or a possible hardware failure.

A complete list of the possible troubleshooting steps that should be performed to resolve this issue include:

- Checking the cable connections.
- Resetting the equipment.
- Checking the CD LED on the CSU/DSU.
- Reporting the issue to the leased-line provider.
- Replacing the faulty equipment.

The router configuration is not a possible issue in this scenario because both serial 0 and line protocol are down, indicating a problem in the physical layer. Configuration issues, such as an incorrect IP address, would be indicated in the second section of the output (line protocol is up/down). The second section, regardless of whether it says up or down is meaningless when the first section indicates a problem.

You should not check the router configuration for the shutdown interface command. When an interface has been manually shut down with this command, it will be indicated in the output as Serial 0 is administratively down, line protocol is down.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

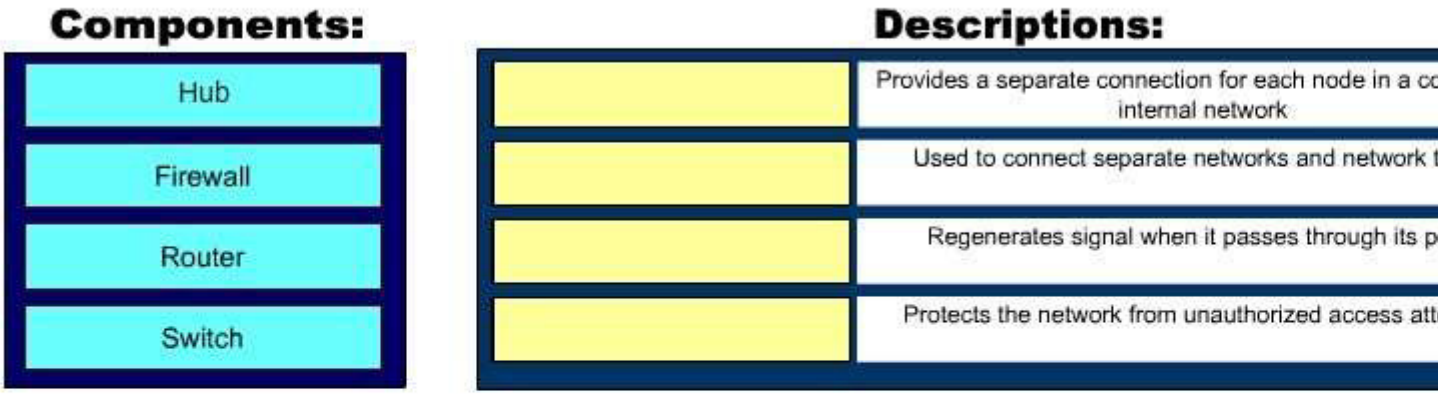
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book.html

https://www.cisco.com/c/en/us/products/collateral/routers/1700-series-modular-access-routers/prod_end-of-life_notice0900aecd8044473f.html

QUESTION 91
DRAG DROP
Click and drag the network devices from the left to their appropriate descriptions on the right.

Select and Place:

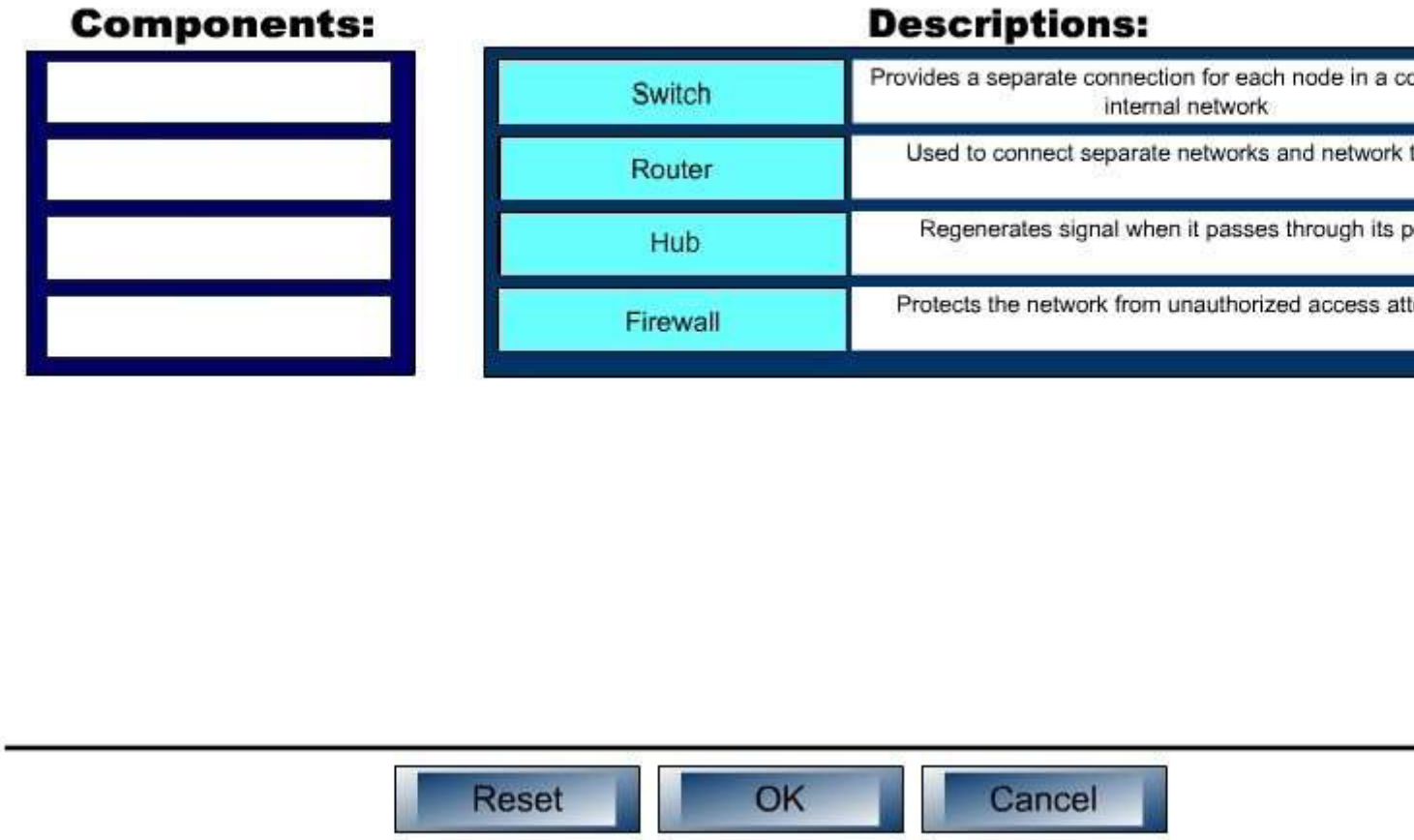
Note: You must press the 'OK' button below to record your responses.



Reset OK Cancel

Correct Answer:

Note: You must press the 'OK' button below to record your responses.

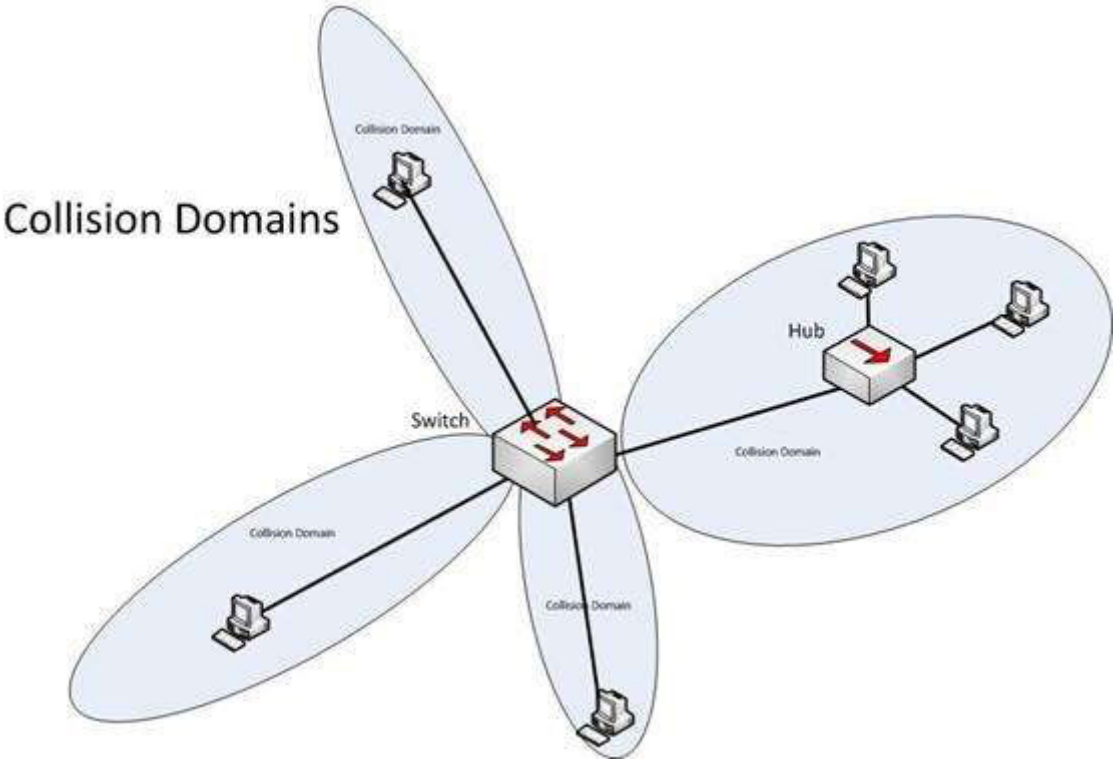


Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following are some of the network devices and their corresponding functions:

- Hub: Regenerates a signal when it passes through its ports. Hubs provide a common connection point for network devices. Hubs are generally used for LAN connectivity and works at Layer 1 of the OSI model.
- Firewall: Protects the network from unauthorized access attempts. It is typically placed between the Internet and aprivate network, but can also be placed between two private networks.
- Router: Provides a means for connecting LAN and WAN segments together. A router separates broadcast domains while connecting different logical and physical networks.
- Switch: Provides a separate collision domain for each node in a company's internal network. Switches work at Layer 2 in the Open System Interconnection (OSI) model and perform their function by observing the source and destination MAC addresses of packets. Because of this method of operation, it can provide dedicated bandwidth to each connected node. Advantages of switches over hubs include the ability to filter frames based on MAC addresses and to allow simultaneous frame transmissions. The diagram below illustrates the ability of a switch to provide a separate collision domain to each device, as compared to the hub, which cannot.



Objective:
Network Fundamentals

Sub-Objective:
Describe the impact of infrastructure components in an enterprise network

References:

http://docwiki.cisco.com/wiki/Internetwork_Design_Guide

QUESTION 92
Examine the following partial output of the show interfaces command.

Router# show interfaces ethernet 0/0
Ethernet0/0 is administratively down, line protocol is down
Hardware is AmdP2, address is 0003.e39b.9220 (bia 0003.e39b.9220)
Internet address is 10.1.0.254/16
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
<<output omitted>>

Which of the following statements are true? (Choose all that apply.)

A. the interface is functional
B. the largest frame allowed through this connection is 1500 bytes
C. the interface needs the no shutdown command executed to be functional
D. the largest frame allowed through this connection is 10000 Kbs

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference:
Explanation:

From this output, we can determine that the largest frame allowed through this connection is 1500 bytes and that the interface needs the no shutdown command executed to be functional. The portions of the output that tell us this are:

MTU 1500 bytes indicates that the Maximum Transmission Unit (MTU) is 1500 bytes. The MTU is the largest frame size allowed.

Ethernet0/0 is administratively down indicates that the interface has either been disabled or has never been enabled. The command no shutdown is used to enable an interface, and until enabled, it will not function.

The interface is not functional, as indicated by the Ethernet0/0 is administratively down portion of the output.

The largest frame allowed through this connection is not 10000 Kbs.It is 1500 bytes. It is interesting to note that the bandwidth of the connection is 10000 Kbs, as indicated by the section:

BW 10000 Kbit

Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors,duplex, speed)

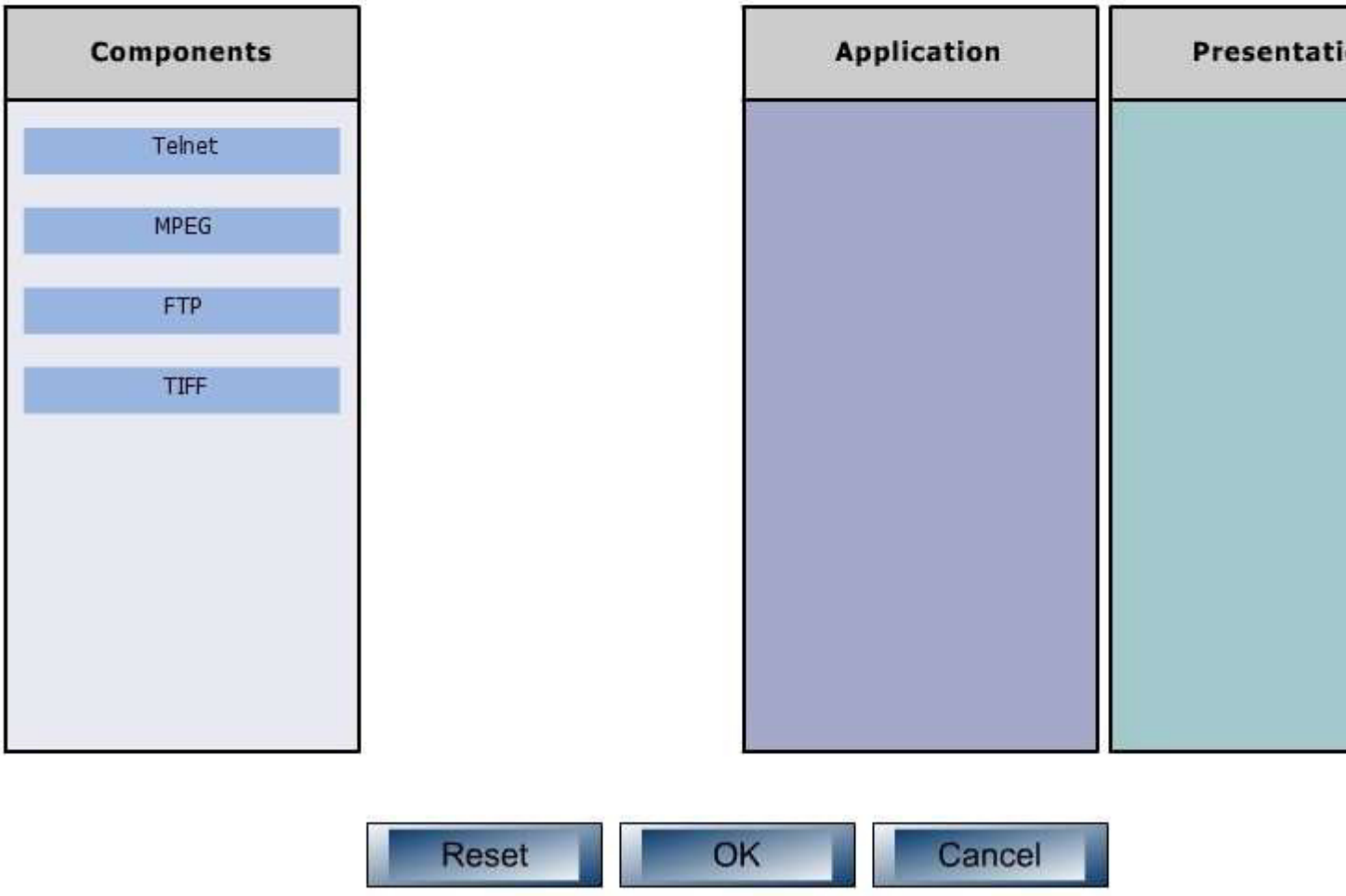
References:

https://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/eos-eol-notice-listing.html

QUESTION 93
DRAG DROP
Click and drag the components on the left to their corresponding layers of the Open Systems Interconnection (OSI) model on the right.

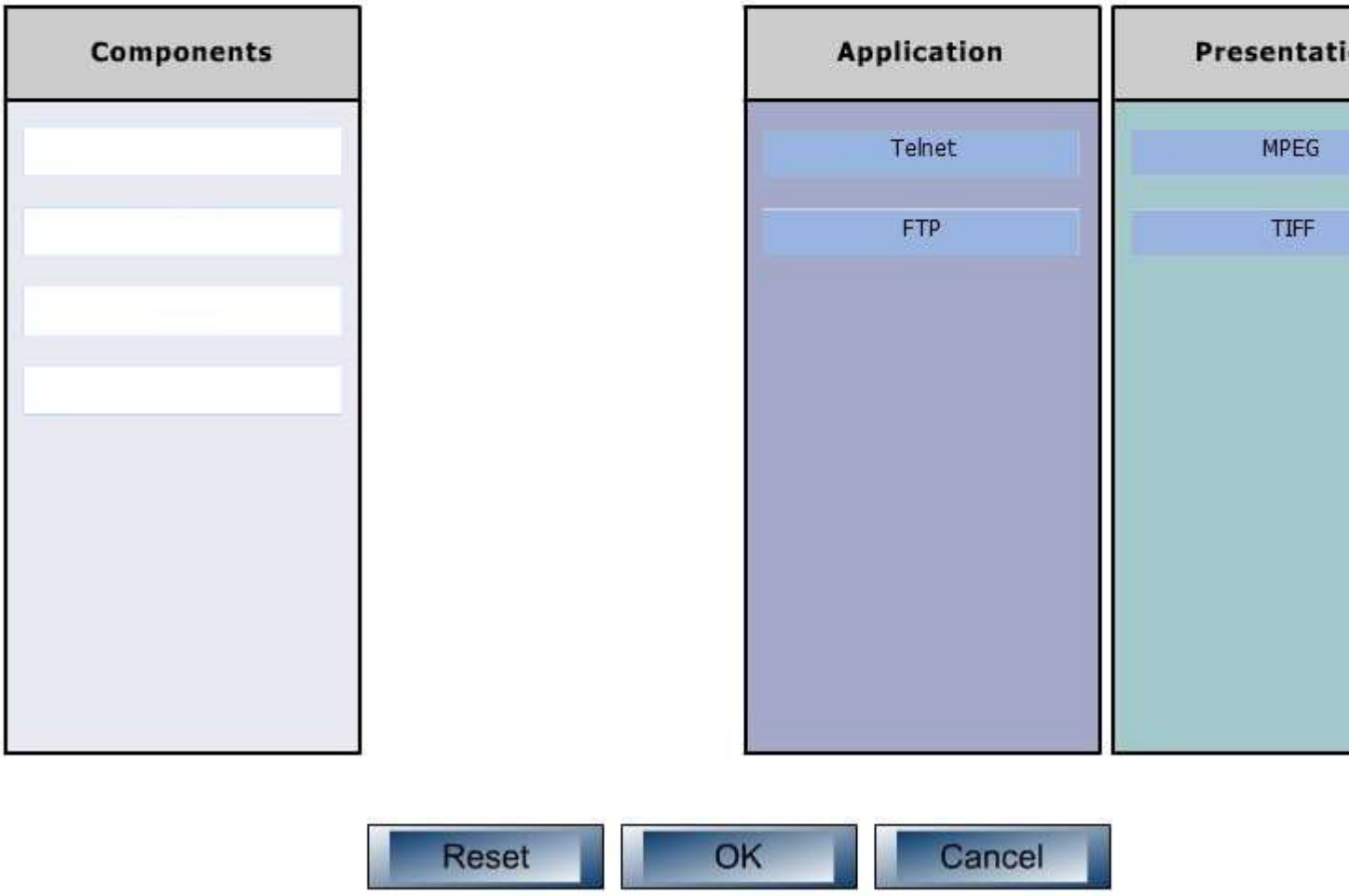
Select and Place:

Note: You must press the 'OK' button below to record your responses.



Correct Answer:

Note: You must press the 'OK' button below to record your responses.



Section: (none)
Explanation

Explanation/Reference:
Explanation:

File Transfer Protocol (FTP) and Telnet are services, which are implemented at the Application layer in the Open Systems Interconnection (OSI) model. The Application layer is responsible for interacting directly with the application. It provides application services, such as e-mail.

Motion Picture Experts Group (MPEG) and TaggedImage File Format (TIFF) are graphic image formats, which are implemented at the Presentation layer. The Presentation layer enables coding and conversion functions for application layer data. Data is formatted and encrypted at this layer. The Presentation layer converts data into a format which is acceptable to the Application layer.

The following are also OSI layers and their descriptions:

- Session: Used to create, manage, and terminate sessions between communicating nodes. The Session layer handles the service requests and service responses which take place between different applications.
- Transport: Responsible for error-free and sequential delivery of data. This layer is used to manage data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Network: Used to define the network address or the Internet Protocol (IP) address, which is then used by the routers to make routing decisions.
- Data Link: Ensures the reliable transmission of data across a network on the basis of Layer 2 addresses such as MAC addresses (Ethernet) or DLCIs (Frame relay).
- Physical: Consists of hardware for sending and receiving data on a carrier. The protocolswhich work at the Physical layer include Fast Ethernet, RS232 and Asynchronous Transfer Mode (ATM).

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast OSI and TCP/IP models

References:

http://docwiki.cisco.com/wiki/Internetworking_Basics#OSI_Model_and_Communication_Between_Systems

QUESTION 94
The conference room has a switch port available for use by the presenter during classes. You would liketo prevent that port from hosting a hub or switch. Which of the following commands could be used to prevent that port from hosting a hub or switch?

A. switchport port-security maximum
B. switchport port-security mac address sticky
C. switchport port-security mac address
D. switchport port-security

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The switchport port-security command would prevent the port from hosting a hub or switch. This command enables port security on an interface. It does not specify a maximum number of MAC addresses, but in the default is 1, therefore it would accomplish the goal.

The switchport port-security maximum command alone could not be used to limit the number of MAC addresses allowed on the interface to 1. This command has no effect unless the switchport port-security command has been executed.

The switchport port-security mac address sticky command would not prevent that port from hosting a hub or switch. This command is used to allow a port to dynamically learn the first MAC address it sees in the port, add it to the MAC address table and save it to the running configuration of the switch.

The switchport port-security mac address command would not prevent that port from hosting a hub or switch. This command is used to manually assign a MAC address to a port as a secure address. When used in combination with the switchport port-security maximum command, the use of the port can not only be limited to one address at a time, but also limited to only a specific address. For example, the following set of commands

would assure that only the device with the MAC address of 0018.cd33.46b3 will be able to connect to the port:

Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0018.cd33.46b3

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot port security

References:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ewa/configuration/guide/conf/port_sec.html

QUESTION 95
What command was used to generate the output shown below?

Connection-specific DNS Suffix . : ajax.acme.com
Description . . . .: Broadcom NetXtreme 57xx Gigabit Controller

Physical Address. . . . . : 00-1A-A0-E1-95-AB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . : fe80::ada3:8b73:a66e:6bc0%10(Preferred)
IPv4 Address. . . . . : 10.88.2.177(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . .. : Wednesday, October 05, 2011 4:31:32 PM
Lease Expires . . . . . : Friday, October 07, 2011 4:33:32 AM
Default Gateway . . . . . : 10.88.2.6
DHCP Server . . . . . : 10.88.10.48
DHCPv6 IAID . . . . . : 234887840
DHCPv6 Client DUID. . . : 00-01-00-01-14-EE-0F-98-00-1A-A0-E1-95-AB

DNS Servers . . . . . : 10.88.10.48
10.75.139.18
NetBIOS over Tcpip. . . . . : Enabled

A. winipcfg
B. ipconfig
C. ifconfig
D. ipconfig/all

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The output displayed is that generated by the ipconfig/all command as executed on a Windows computer. This command displays a wealth of information about the current configuration. Examples of information that can be gleaned from the sample output include:

- The router for computer is at 10.88.2.6.
- The primary DNS server is 10.88.10.49.
- The address of the computer is 10.88.2.177. Any packets that need tobe sent to any computers in the

10.88.2.0/24 network will not use the default gateway but will be switched to the destination by MAC address. Packets that need to be sent to any other network, however, will require the use of the default gateway and so the frame will be switched to MAC address of the gateway.

This information can be used with other utilities for troubleshooting. For example, if you can ping the primary DNS server at 10.88.10.49, which in a remote network, then the IP address is correct and your router (10.88.2.6) knows a route to the network where the DNS server is located. However, this result would NOT prove that DNS is working correctly. Verification would require successfully pinging local or remote hosts by name rather than IP address.

It is not the output of winipcfg. This command was used in Windows 95 to generate a subset of this information in a GUI dialog box.

It is not the output of ifconfig. This command is used to generate a subset of this information in a Linux/Unix environment.

It is not the output of ipconfig. This command generates IP address subnet mask and gateway only.

Objective:
Network Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

QUESTION 96
Which feature enables a host to obtain an IP address from a DHCP server on another subnet?

A. DHCP relay agent
B. DHCP BOOTP agent
C. DHCP relay protocol
D. DHCP BOOTP relay

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A Dynamic Host Configuration Protocol (DHCP) relay agent enables hosts to obtain IP addresses from a DHCP server on another subnet. Hosts use DHCPDISCOVER broadcast messages to locate the DHCP server because they don't know the location of the DHCP server. Because routers are designed to filter broadcasts, the DHCPDISCOVER packet would be dropped unless the router is configured to forward such packets. Enabling a DHCP relay agent on a Cisco router allows it to receive certain types of broadcasts and forward them to special helper addresses.

The following sequence describes an IP address relay process:

- The DHCP client broadcasts a DHCP request on the network.
- The DHCP request is intercepted by the DHCP relay agent, which inserts the relay agent information option (option 82) in the packet.
- The DHCP relay agent forwards the DHCP packet to the DHCP server.
-The DHCP server uses the suboptions of option 82 in the packet, assigns IP addresses and other configuration parameters, and forwards the packet to the client.
- The relay agent again intercepts the packet and strips off the option 82 information before sending it to the

client.

The ip helper-address interface configuration command enables a DHCP relay agent on a Cisco router.

DHCP is an enhancement over Bootstrap Protocol (BOOTP) and is used to automate the distribution of IP address to clients from a central server. The BOOTP protocol was also used distribute IP addresses, but was inflexible to changes in the network. DHCP offers three advantages that also address the inflexibility of the BOOTP protocol:

- Automatic allocation of permanent IP addresses
- Automatic allocation of time bound (leased) IP addresses
- Ability to assign static IP address or define a pool of reserved IP address

When a DHCP relay is unnecessary, the following steps describe the address allocation process:

- The client device broadcasts a DHCPDISCOVER broadcast message to locate a DHCP server.
- The DHCP server replies with a DHCPOFFER unicast message containing configuration parameters, such as an IP address, a MAC address, a domain name, and a lease for the IP address for theclient device.
- The client sends back a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the DHCP server.
- The DHCP server replies back to client device with DHCPACK unicast message, acknowledging the allocation of the IP address to this client device.

While DHCP is very useful in reducing the administrative burden of issuing IP configurations in a large network, Cisco best practices call for using static IP addressing in a small (6 or fewer hosts) network.

All other options are invalid devices or features.

Objective:
Infrastructure Services

Sub-Objective:
Troubleshoot client- and router-based DHCP connectivity issues

References:

https://www.cisco.com/c/en/us/products/index.html

https://www.cisco.com/c/en/us/td/docs/ios/ipapp/command/reference/iap_i1.html#wp1032599

QUESTION 97
You have successfully configured a router, but it prompts you to run Setup mode every time the router is restarted. Based on the following output, what could be causing this problem?

RouterA# show version

Cisco Internetwork Operating System SoftwareIOS (tm) 2500 Software (C2500-JS-L), Version 11.3(6), RELEASE SOFTWARE (fc1)

Copyright 1986-1998 by Cisco Systems, Inc.
Compiled Tue 06-Oct-98 22:17 by kpma
Image text-base: 0x03048CF4, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)

RouterA uptime is 25 minutes
System restarted by power-on
System image file is "flash:c2500-js-l_113-6.bin", booted via flash

Cisco 2500 (68030) processor (revision D) with 4096K/2048K bytes of memory.
Processor board ID 04203139, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2142

A. The router does not have sufficient flash memory.
B. The configuration register is incorrect.
C. The configuration file could not be found in NVRAM.
D. The router could not locate a configuration file over the network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The configuration register is incorrect. The configuration register value of 2142 is preventing the router from loading the configuration file from NVRAM.

The router configuration register is used to control various aspects of the router boot sequence, and defaults to a value of 2102. A configuration register of2102 indicates that the router should boot normally, which consists of loading the Internetwork Operating System (IOS) into RAM, then loading the saved configuration file from Non-Volatile RAM (NVRAM) to configure the router.

Changing the configuration register to 2142 tells the router to bypass the saved configuration in NVRAM. This causes the router to boot with a default running configuration, and prompt to run the Initial Configuration Dialog (or Setup mode). Changing the configuration register to 2142is necessary to perform password recovery or to bypass any other aspect of a saved configuration that might be causing problems. After the situation is resolved, the configuration register would then be changed back to the default of 2102 with the following command:

Router(config)# config-register 0x2102

The router is successfully loading the IOS from flash memory, so insufficient flash memory is an incorrect answer.

The configuration register is instructing the router to bypass the configuration file in NVRAM, so it is incorrect to state that the configuration file could not be found in NVRAM.

The configuration register is instructing the router to bypass the configuration file in NVRAM, so it is incorrect to state that the router could not locate a configuration file over the network.

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:

https://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html

https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_c1.html#wp1068966

QUESTION 98
RouterA and RouterB, which connect two locations, are unable to communicate. You run the show running-configuration command on both router interfaces, RouterA and RouterB. The following is a partial output:

```
routerA#show running-config
interface Serial0
description Router_A
ip address 192.10.191.2 255.255.255.0
encapsulation ppp
no ip mroute-cache
clockrate 64000

routerB#show running-config
interface Serial1
description Router_B
ip address 192.10.192.1 255.255.255.0
encapsulation ppp
no ip mroute-cache
clockrate 64000
```

Based on the information given in the output, what are two likely causes of the problem? (Choose two.)

A. The IP address defined is incorrect.
B. Both routers cannot have a clock rate defined.
C. Both routers cannot have an identical clock rate.
D. The Layer 2 framing is misconfigured.
E. At least one of the routers must have the ip mroute-cache command enabled.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Two possible causes of the problem are that the IP addresses are incorrect as defined, or that both routers have a defined clock rate. The IP addresses on the routers are in different subnets. The IP addresses need to be changed to fall in the same subnet.

Both routers cannot have a clock rate configured. Only routers with a DCE cable connected should have a clock rate, which provides synchronization to the router connected to the DTE cable. In a point-to-point serial connection, the DCE cable connects to the DTE cable, providing a communication path between the two routers. If both computers have a clock rate configured, the routers will not communicate.

A matching clock rate is not the problem. The clock rates between two routers should match. The router connected to the DCE cable will provide the clock rate to the router connected to the DTE cable, resulting in matching clock rates.

The Layer 2 encapsulation refers to the Data Link protocol used on the link. In this case, the protocol is Point to Point Protocol (PPP), which is configured correctly on both ends as indicated by the matching encapsulation ppp statements in the output. The connection would be prevented from working if one of the routers were missing this setting (which would be indicated by the absence of the encapsulation ppp statement in its output), or if a different Layer 2 encapsulation type were configured, such as High-Level Data Link Control (HDLC).

The ip mroute-cache command is used to fast-switch multicast packets and would not cause the problem in this scenario.

Objective:
Network Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

http://docwiki.cisco.com/wiki/Point-to-Point_Protocol

https://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

QUESTION 99
You need to manually assign IPv6 addresses to the interfaces on an IPv6-enabled router. While assigning addresses, you need to ensure that the addresses participate in neighbor discovery and in stateless auto-configuration process on a physical link.

Which of the following addresses can be assigned to the interfaces?

A. FEC0:0:0:1::1/64
B. FE80::260:3EFF:FE11:6770/10
C. 2001:0410:0:1:0:0:0:1/64
D. 2002:500E:2301:1:20D:BDFF:FE99:F559/64

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The FE80::260:3EFF:FE11:6770/10 address can be assigned to an interface of the IPv6-enabled router. This address is a link-local address as it has the prefix FE80::/10. Link-local addresses can be configured for an interface either automatically or manually.

Link-local addresses are IPv6 unicast addresses that are configured on the interfaces of an IPv6-enabled router. With link-local addresses, the nodes can connect to a network (local link) and communicate with other nodes. In addition, these addresses participate in the neighbor discovery protocol and the stateless auto-configuration process.

The FEC0:0:0:1::1/64 address should not be used for the interfaces because this address is a site-local address. Site-local addresses are IPv6 equivalent addresses to IPv4's private address classes. These addresses are available only within a site or an intranet, which typically is made of several network links.

You should not use the 2001:0410:0:1:0:0:0:1/64 and 2002:500E:2301:1:20D:BDFF:FE99:F559 addresses for the interfaces. These two addresses are global unicast addresses as they fall in the range from 2000::/3 and to E000::/3. A global address is used on links that connect organizations to the Internet service providers (ISPs).

Objective:
Network Fundamentals

Sub-Objective:
Configure and verify IPv6 Stateless Address Auto Configuration

References:

https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-lla.html

QUESTION 100
Two catalyst switches on a LAN are connected to each other with redundant links and have Spanning Tree Protocol (STP) disabled. What problem could occur from this configuration?

A. It may cause broadcast storms.
B. All ports on both switches may change to a forwarding state.
C. It may cause a collision storm.
D. These switches will not forward VTP information.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The configuration in the scenario may cause broadcast storms. When there are redundant links between two switches, it is recommended that you enable Spanning Tree Protocol to avoid switching loops or broadcast storms. Loops occur when there is more than one path between two switches. STP allows only one active path at a time, thus preventing loops. A broadcast storm occurs when the network is plagued with constant broadcasts. When the switches have redundant links, the resulting loops would generate more broadcasts, eventually resulting in a complete blockage of available bandwidth that could bring the complete network down. This situation is referred to as a broadcast storm.

The option stating that all ports on both switches may change to a forwarding state is incorrect. Forwarding is a port state that is available when using STP. When STP is disabled, the switch cannot change the STP states of its ports.

The option stating that the switches will not forward VLAN Trunking Protocol (VTP) information is incorrect. Enabling or disabling STP does not have a direct effect on VTP messages.

The term collision storm is not a valid term.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot interswitch connectivity

References:

https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/12006-chapter22.html#spans

QUESTION 101
Which command would you use to see which interfaces are currently operating as trunks?

A. show interface switchports
B. show trunk interface
C. show interfaces trunk
D. show switchport trunk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show interfaces trunk command displays a list of interfaces currently operating as trunks, and their configuration (such as supported VLANs or frame tagging method). Sample output would resemble the following:

Switch# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gi0/1 desirable 802.1q trunking 1
Gi0/2 desirable 802.1q trunking 1

Port Vlans allowed on trunk
Gi0/1 1-4094
Gi0/2 1-4094
<<output omitted>>

This output indicates that switch ports Gi0/1 and Gi0/2 are both currently operating as trunks (Status), and that 802.1q frame tagging is being used on the trunk links.

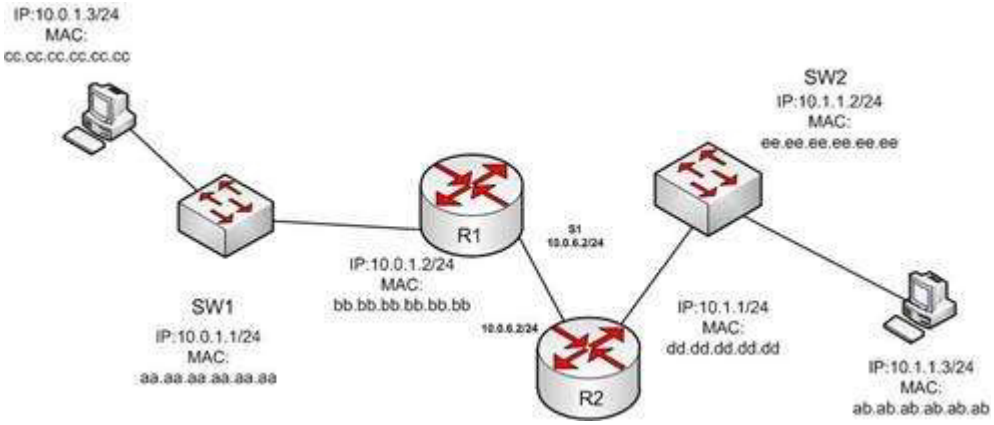
The remaining options are incorrect because they are not valid Cisco IOS commands.

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book.html

QUESTION 102
In the diagram below, if the workstation at 10.0.1.3 sends a packet to the workstation at 10.1.1.3, what will be the source physical address when the packet arrives at 10.1.1.3?



A. ab.ab.ab.ab.ab.ab
B. ee.ee.ee.ee.ee.ee
C. dd.dd.dd.dd.dd.dd
D. cc.cc.cc.cc.cc.cc
E. aa.aa.aa.aa.aa.aa
F. bb.bb.bb.bb.bb.bb

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The source physical address of the packet when it arrivesat 10.1.1.3 will be that of the interface on the R2 router, dd.dd.dd.dd.dd.dd . Each router will change the MAC address field to the MAC address of its sending interface as it sends the packet and will leave the IP address field unchanged. The switches will change neither field, but will simply use the MAC address field to determine the forwarding path and switch the frame to the port where the MAC address is located. The R2 router is the last device that will make a change to the MAC address field.

The source (10.0.1.3) and destination (10.1.1.3) IP address fields will stay the same at each device. The MAC address field changes when R1 sends the frame to R2 and when R2 send the frame to the workstation at 10.1.1.3.

Objective:
LAN Switching Fundamentals

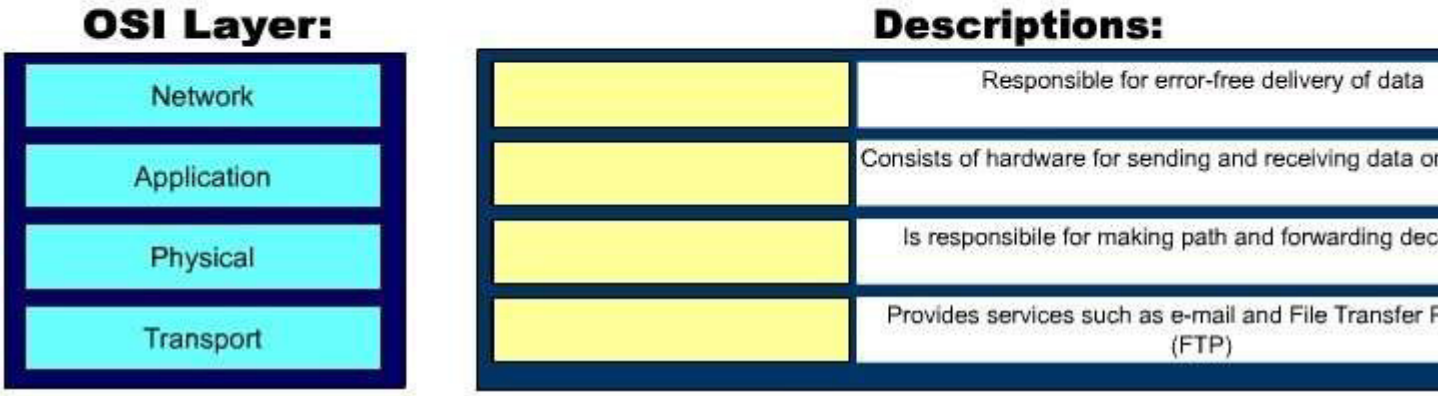
Sub-Objective:
Describe and verify switching concepts

References:
http://docwiki.cisco.com/wiki/Routing_Basics

QUESTION 103
DRAG DROP
Click and drag the Open Systems Interconnection (OSI) layers to their corresponding functions on the right.

Select and Place:

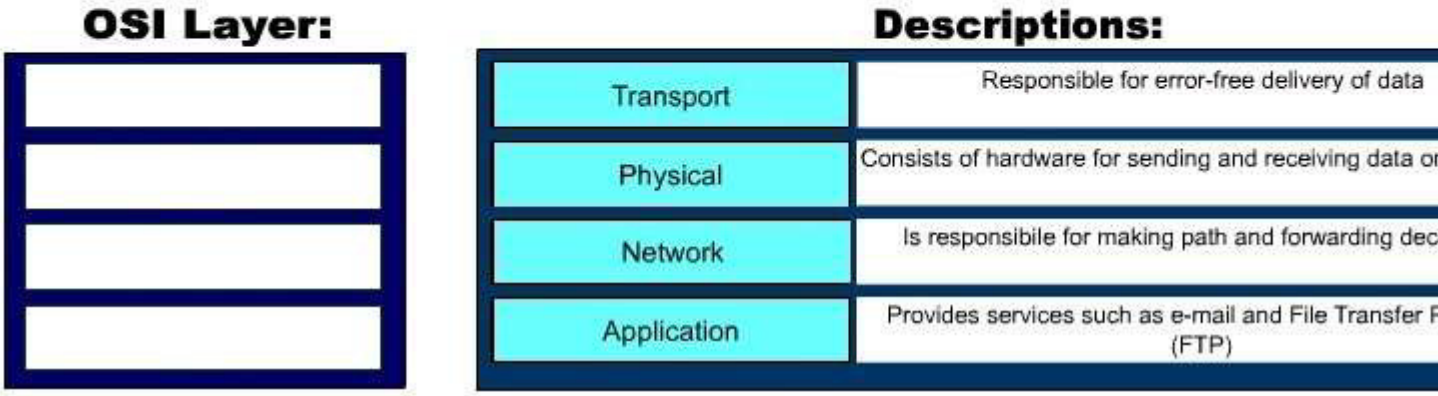
Note: You must press the 'OK' button below to record your responses.



Reset OK Cancel

Correct Answer:

Note: You must press the 'OK' button below to record your responses.



Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following are the OSI layers along with their descriptions:

- Application: Responsible for interacting directly with the application. It provides application services such as e-mail and File Transfer Protocol (FTP).
- Physical: Consists of hardware for sending and receiving data on a carrier. The protocols which work at the Physical layer include Fast Ethernet, RS232, and Asynchronous Transfer Mode (ATM).
- Transport: Responsible for error-free and sequential delivery of data. This layer is used to manage data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Network: Used to define the network address or the Internet Protocol (IP) address, which is then used by the routers to make routing decisions.
- The following are also OSI layers:
- Presentation: Enables coding and conversion functions for application layer data. The formatting and encryption of data is done at this layer. The Presentation layer converts data into a format which is acceptable by the application layer.

- Session: Used to create, manage, and terminate sessions between communicating nodes. The session layer handles the service requests and service responses, which take place between different applications.
- Data Link: Ensures the reliable transmission of data across a network on the basis of Layer 2 addresses such as MAC addresses (Ethernet) or DLCIs (Frame Relay).

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast OSI and TCP/IP models

References:

http://docwiki.cisco.com/wiki/Internetworking_Basics#OSI_Model_and_Communication_Between_Systems

QUESTION 104
Which of the following statements is TRUE about trunk ports?

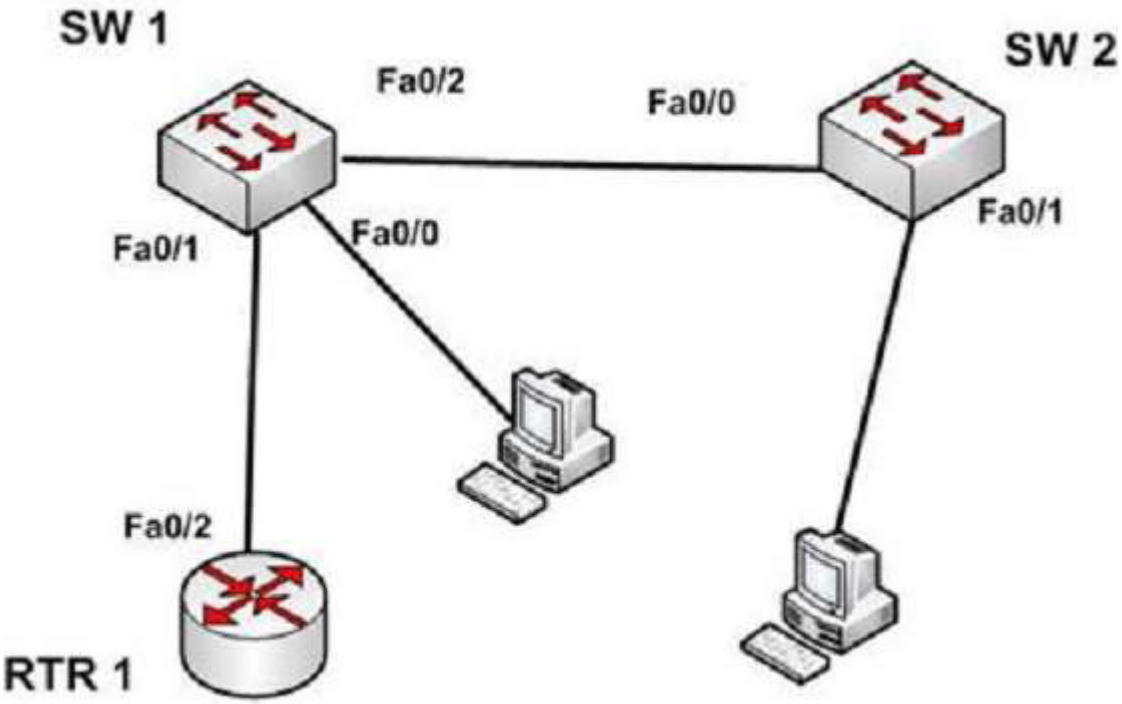
A. A trunk port connects an end-user workstation to a switch.
B. A trunk port uses 802.1q to identify traffic from different VLANs.
C. A trunk port supports a single VLAN.
D. A trunk port uses a straight-through Ethernet cable when connecting two switches.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A switch port can operate as an access port or a trunk port. An access port is used to connect to an end-user device, such as a workstation, server, or printer,while a trunk port is used to connect to neighboring switches or routers. The trunk link is responsible for carrying data between workstations connected to different switches, or a switch and a router configured for inter-VLAN routing. For example, in the diagram below where VLANs are in use on both switches and inter-VLAN routing is configured, the interfaces will operate as follows:

- SW1 - Fa0/1 and Fa0/2 are trunk links, Fa0/0 is an access link
- SW2 - Fa0/0 is trunk link and Fa0/1 is an access link
-RTR - Fa0/2 is a trunk link



With the exception of frames traveling on the native VLAN, data frames crossing a trunk link must be frame tagged over the link to identify the VLAN that sourced the frame. The receiving switch sees the VLAN ID, and uses this information to forward the frame appropriately. 802.1q and ISL are the two possible frame tagging methods between Cisco switches. In summary, some facts about access and trunk ports:

Access ports:

- Carry traffic for a single VLAN
- Connect end user workstations to the switch
- Use a straight-through cable to connect to the device

Trunk ports:

- Facilitate inter-VLAN communication when connected to a Layer 3 device
- Carry traffic from multiple VLANs
- Use 802.1q to identify traffic from different VLANs

When a new trunk link is created on a switch, all VLANs are allowed to use the trunk, by default.

Trunk ports are used between switches and routers, and do not connect to end-user workstations.

Trunk ports support all VLANs known to the switch by default, so that devices in the same VLAN can communicate across multiple switches. Trunk ports are not limited to a single VLAN, as access ports are.

Trunk ports connected between switches using crossover Ethernet cables, not straight-through Ethernet cables. Trunk ports between switches and routers use straight-through cables.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot interswitch connectivity

References:

http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3

QUESTION 105
You have been asked to examine the following output to identify any security problems with the router. Its configuration is shown:

```
Current configuration:
!
version 11.2
!
hostname cisco
!
enable secret 5 $1$mERr$7sOd0mgRuXYhHwfWsV4QZ/
!
banner login ^C Welcome to Router 5 Authorized users only ^C
!
interface Ethernet0
ip address 10.1.1.1 255.0.0.0
!
interface Serial0
ip address 20.2.2.2 255.0.0.0
!
router rip
network 10.0.0.0
network 20.0.0.0
!
ip route 0.0.0.0 0.0.0.0 20.2.2.3
!
line vty 0 4
password Cisc0$ell$
no login
!
end
```

What problems exist? (Choose all that apply.)

A. unencrypted privileged mode password
B. inappropriate wording in the banner message
C. weak password on the VTY line
D. Telnet users will not be prompted for a password

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The banner logon message should not contain verbiage that includes the word Welcome. This could potentially supply grounds by a hacker that he was "invited" to access the device.

Also, although a strong password has been configured on the VTY lines, the presence of the no login command instructs the router to NOT prompt for a password.

The login command should be executed under the VTY configuration so that the router will prompt for the password.

The privileged mode password is encrypted because it is listed as an enable secret password.

The password configured on the VTY lines, Cisc0ell, is strong in that it contains numbers, letters, and non-numeric characters and it is at least 8 characters in length.

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure, verify, and troubleshoot basic device hardening

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf004.html#wp1017507

QUESTION 106
Which show interfaces command output indicates that the link may not be functional due to a Data Link layer issue, while the Physical layer is operational?

A. Ethernet 0/0 is up, line protocol is up
B. Ethernet 0/0 is up, line protocol is down
C. Ethernet 0/0 is down, line protocol is up
D. Ethernet 0/0 is down, line protocol is down

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The first or left-hand column (Ethernet 0/0 is up) indicates the Physical layer state of the interface, while the second or right-hand column (line protocol is down) indicates the Data Link layer state of the interface. The following command output excerpt indicates that the link is not functional due to a Data Link layer (or "line protocol") issue, while the Physical layer is operational:

Ethernet 0/0 is up, line protocol is down

If the problem were at the Data Link layer while the Physical layer is operational, the show interfaces command output will indicate that the interface is up, but the line protocol is down.

In the normal operation mode, when both Physical layer and Data Link layer are up, the show interfaces output will display the following message:

Ethernet0/0 is up, line protocol is up

The message Ethernet 0/0 is down, line protocol is up is not a valid output.

The message Ethernet 0/0 is down, line protocol is down indicating that both the Physical layer and the Data Link layer are down. Therefore, this is an incorrect option.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:
https://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

QUESTION 107
Which Cisco Internetwork Operating System (IOS) command is used to save the running configuration to non-volatile random access memory (NVRAM)?

A. copy startup-config running-config
B. move startup-config running-config
C. copy running-config startup-config
D. move startup-config running-config

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The copy running-config startup-config command is used to save the running configuration to NVRAM. This command will should always been run after making changes to the configuration. Failure to do so will result in the changes being discarded at the next restart of the router. When the router is restarted, the startup configuration file is copied to RAM and becomes the running configuration.

The copy startup-config running-config command is incorrect because this command is used to copy the startup configuration to the running configuration. The command would be used to discard changes to the configuration without restarting the router.

The move startup-config running-config and move startup-config running-config commands are incorrect because these are not valid Cisco IOS commands. There is no move command when discussing the manipulation of configuration files.

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

References:
https://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/mgx_8850/software/mgx_r3/rpm/rpm_r1-1/configuration/guide/appc.html

QUESTION 108
Which two are the limitations of the service password-encryption command? (Choose two.)

A. It uses the MD5 algorithm for password hashing.
B. It uses the Vigenere cipher algorithm.
C. An observer cannot read the password when looking at the administrator's screen.
D. The algorithm used by this command cannot protect the configuration files against detailed analysis by attackers.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following are limitations of the service password-encryption command:

- It uses the Vigenere cipher algorithm, which is simple in nature.
- A cryptographer can easily crack the algorithm in a few hours.
- The algorithm used by this command cannot protect the configuration files against detailed analysis by attackers.

The service password-encryption command does not use the MD5 algorithm for password hashing. The MD5 algorithm is used by the enable secret command.

The option stating that an observer cannot read the password when looking at the administrator's screen is incorrect because this is an advantage of the service password-encryption command.

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure, verify, and troubleshoot basic device hardening

References:

https://www.cisco.com/c/en/us/support/index.html

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

QUESTION 109
You know that Router2 is configured for RIP. Which Cisco Internetwork Operating System (IOS) command is used to view the current state of all active routing protocols?

A. show ip arp
B. debug ip rip
C. show ip protocols
D. show ip routing process
E. show arp
F. show interfaces

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show ip protocols command is used to view the current state of active routing protocols. This command is issued from Privileged EXEC mode. The syntax of the command is as follows:

```
Router2# show ip protocols
```

Output of the command would resemble the following:

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 2 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
Ethernet0 2 2 trees
Fddi0 2 2
Routing for Networks:
201.19.0.0
16.2.0.0
10.3.0.0
Routing Information Sources:
Gateway Distance Last Update
201.19.0.9 120 00:00:25
16.2.0.10 120          00:03:10
10.33.0.15 120 00:00:57
Distance: (default is 120)
```

This command shows additional information about individual protocols. The version number of RIP being used is shown on the seventh line of the output. This output also indicates on lines 12-14 that it is routing for three networks: 201.19.0.0, 16.2.0.0, and 10.3.0.0. This means that the router will be sending and receiving RIP updates on any interfaces that have IP addresses in those networks.

Also note that the router at 16.2.0.10 has not sent an update in 3 minutes and 10 seconds. If an update is not received in 50 seconds (for a total of 4 minutes), the route-flush timer (240 seconds from the last valid update) will have expired, causing the local router to remove all networks learned from the router at 16.2.0.10 from the routing table.

For more specific information about those interfaces, in terms such as S0 or Fa0/0, you could execute the show ip interface brief command as shown below. The output displays the addresses of the interfaces, which would indicate which interfaces were enabled for RIP and thus sending and receiving updates.

Router# show ip interface brief
Interface IP-Address OK? Method Status
Fastethernet0/0 201.19.0.8 Yes manual up
Serial0/0 16.2.0.1 Yes manual up
Serial0/1 10.33.0.9 Yes manual up

The show ip arp command is incorrect because this command is executed on a router to determine the IP and MAC addresses of hosts on a LAN connected to the router.

The debug ip rip command is incorrect because this command is used to capture RIP traffic between the routers in real time. This command could also be used to determine the version of RIP being used as shown in line 2 of the partial output of the command below:

Router2#debug ip rip
RIP protocol debugging is on

*Mar 3 02:11:39.207:RIP:received packet with text authentication 234
*Mar 3 02:11:39.211:RIP:received v1 update from 122.108.0.10 on Serial0

*Mar 3 02:11:39.211:RIP: 79.0.0.0/8 via 0.0.0.0 in 2 hops
*Mar 3 02:11:40.212:RIP: ignored v2 packet from 192.168.5.6 (illegal version)

In the above output Router 2 has received a version 1 update from a router at 122.108.0.10 which indicates that a ping to that router should succeed. It also shows what was learned from the router at 122.108.0.10, which is the router to network 79.0.0.0/8 via 0.0.0.0. The 0.0.0.0 indicates that the next hop for that route is the router that sent this advertising (the router at 122.108.0.10).

The output also shows that a RIP router at 192.168.5.6 sent a version 2 update that was ignored by Router 2, which is using version 1. This mismatch of versions will prevent Router 2 from forming an adjacency with the router at 192.168.5.6.

Note: Before running any debug command you should execute the show processes command and verify that the CPU utilization on the router is low enough to handle the effects of running the debug command.

The show ip routing process command is incorrect because it is not a valid Cisco IOS command.

The show arp command is used to identify the IP address to MAC address mappings the router has leaned through the ARP broadcast process. It is helpful when you have identified errors associated with a MAC address and you need to learn the IP address or vice versa. Sample output is below.

router# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.0.0.3 0 0004.dd0c.ffcb ARPA Ethernet01
Internet 10.0.0.1 - 0004.dd0c.ff86 ARPA Ethernet0

The difference between the show arp command and the show ip arp command is that show arp will also include mappings learned throughnon-IP protocols such as when inverse ARP is used to learn and map DLCIs to IP addresses.

The show interface command can also be used to identify IP addresses from MAC addresses and vice versa, but also indicates the state of the interface; IP addresses MTU and much more about each interface. Sample output is below.

router# show interfaces
Ethernet 0 is up, line protocol is up
Hardware is MCI Ethernet,address is 0000.0c00.750c(bia 0000.0c00.750c)
Internet address is 10.108.28.8, subnet mask is255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Objective:
Routing Fundamentals

Sub-Objective:
Interpret the components of routing table

References:

https://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfindp2.html#wp1022264

QUESTION 110
Which three statements are TRUE regarding static route assignments? (Choose three.)

A. A single static route cannot respond to network outages.
B. Static routes respond to network outages.
C. Static routes are used to discover the network destinations automatically.
D. Static routes are removed from the routing table if the interface goes down.
E. Static routes are not removed from the routing table if the interface goes down.
F. Static routes are manually configured on the router.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following statements are true regarding static route assignments:

- A single static route cannot respond to network outages.
- Static routes are removed from the routing table if the interface goes down.
- Static routes are manually configured on the router.
- Static routes have several advantages over dynamic routing, including the following:
- No routing protocol overhead is generated by the router if static routes are configured.
- No bandwidth is consumed by route advertisements between network devices.
- Router resources are more efficiently used.
- Network security is increased by using static routes.

The option stating that static routes respond to the network outages is incorrect because static routes do not respond to network outages.

The option stating that static routes are used to discover the network destinations automatically is incorrect because dynamic routing protocols are used to discover the network destinations automatically.

The option stating that static routes are not removed from the routing table if the interface goes down is incorrect. Static routes are removed from the routing table if the necessary interface goes down and the destination network is unreachable.

Objective:
Routing Fundamentals

Sub-Objective:
Compare and contrast static routing and dynamic routing

References:

http://docwiki.cisco.com/wiki/Routing_Basics#Algorithm_Types

QUESTION 111
A device has an address of 192.168.144.21 and a mask of 255.255.255.240. What will be the broadcast address for the subnet to which this device is attached?

A. 192.168.144.23
B. 192.168.144.28
C. 192.168.144.31
D. 192.168.144.32

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The broadcast address for the subnet to which this device is attached will be 192.168.144.31.

To determine the broadcast address of a network where a specific address resides, you must first determine the network ID of the subnetwork where the address resides. The network ID can be obtained by determining the interval between subnet IDs. With a 28-bit mask, the decimal equivalent of the mask will be

255.255.255.240. The interval between subnets can be derived by subtracting the value of the last octet of the mask from 256. In this case, that operation would be 256 - 240. Therefore, the interval is 16.

The first network ID will always be the classful network you started with (in this case 192.168.144.0). Then each subnetwork ID in this network will fall at 16-bit intervals as follows:

192.168.144.0
192.168.144.16
192.168.144.32
192.168.144.48

At 192.168.144.48 we can stop, because the address that we are given as a guide is in the network with a subnet ID of 192.168.144.16. Therefore, since the broadcast address for this network will be 1 less than the next subnet ID (192.168.144.32), the broadcast address for the subnet to which this device is attached is 192.168.144.31.

All the other options are incorrect because none of these will be the broadcast address for the subnet to which this device is attached.

Objective:
Network Fundamentals

Sub-Objective:
Applytroubleshooting methodologies to resolve problems

References:

https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html#ustand_ip_add

QUESTION 112
A user in your network is having trouble accessing resources and the Internet. You decide to examine the partial output of the ipconfig/all command on his machine. The output is shown below:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\TroyMcClure > ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : KREMLIN0120
   Primary Dns Suffix  . . . . . . . : kappa.alpha.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : kappa.alpha.com

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : triad.rr.com
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-N 7260
   Physical Address. . . . . . . . . : F8-16-54-12-E3-69
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DNS Servers . . . . . . . . . . . : 192.168.0.50
```

Which of the following statements describes the user's problem?

A. The default gateway address is incorrect
B. The IP address of the device is incorrect
C. There is no DNS server configured
D. IP routing is not enabled

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The IP address of the device is incorrect. It is not in the same subnet as the default gateway address. While it is possible that the default gateway address is incorrect, that is not as likely a reason, given the fact that the DNS server is also in the same IP subnet as the default gateway.

There is a DNS server configured and its IPaddress is 192.168.0.50. If a DNS server were not configured, this user would be unable to access the Internet, even if all IP addressing problems were resolved.

IP routing is NOT enabled. However, it is not required to be enabled because this device is not acting as a router. The device does not need IP routing enabled to access resources and the Internet if all other IP addressing issues are resolved.

Objective:
Infrastructure Services

Sub-Objective:

Describe DNS lookup operation

References:

http://networking.nitecruzr.net/2005/05/reading-ipconfig-and-diagnosing.html

QUESTION 113
Which command(s) will enable you to configure only serial interface 0 on a Cisco router?

A. router>interface serial 0
B. router#interface serial 0
C. router(config)#interface serial 0
D. router(config-if)#interface serial 0

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You can use either the router(config)# interface serial 0 command or the router(config-if)# interface serial 0 command to configure serial interface 0 on the router. To perform configuration changes on a single interface, you must either enter interface configuration mode for that interface, or simply execute the command to enter configuration mode for another interface while still at the configuration prompt for the previous interface.

Router configuration mode (as indicated by the prompt router(config)#) allows global configuration of the router. This mode, also referred to as the global configuration mode, must be entered as a precursor to entering the interface configuration mode for a specific interface. The sequence of commands and prompts to arrive at this mode would be:

Router> enable (enters privileged mode)
Router#config t (enters global configuration mode, t is short for terminal)
Router(config)# interface serial 0 (enters interface configuration mode for the serial 0 interface)
Router(config-if)#

At this point, any commands executed would be configuration changes limited to the serial 0 interface. For example, to place an address on the interface, enable the interface, and save the configuration, the command series and prompts would be:

Router> enable
Router# config t
Router(config)# interface serial 0
Router(config-if)# ip address 192.168.20.1 255.255.255.0 (addresses the interface)
Router(config-if)# no shutdown (enables or "turns on" the interface)
Router(config-if)# exit (exits global configuration mode)
Router(config)# exit (exits privileged mode)
Router# copy running-config startup config (copies the changes to the configuration file on the router)

Alternately, you could enter interface configuration mode for one interface while still in configuration mode for another interface, as shown below. After entering the interface serial 1 command, you will be editing serial 1 instead of serial 0.

Router(config)# interface serial 0
Router(config)#
Router(config)# interface serial 1

You should not use the command router> interface serial 0. User EXEC mode, as indicated by the prompt router>, provides limited access to a router and is the initial mode you see after authenticating to the router. The

subcommand interface serial 0 is not functional before you proceed to global configuration mode and interface configuration mode for a specific interface.

You should not use the command router# interface serial 0. Privileged mode (as indicated by the prompt router#) must be traversed to get to global configuration mode before you can execute the subcommand interface serial0. This subcommand is not functional while you are still in privileged mode.

Objective:
Infrastructure Maintenance

Sub-Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:

https://search.cisco.com/search?query=Cisco%20IOS%20IP%20Routing%20BFD%20Configuration%20Guide&locale=enUS&tab=Cisco

https://www.cisco.com/c/en/us/obsolete/routers/cisco-1600-series-routers.html

QUESTION 114
Which Cisco Internetwork Operating System (IOS) command is used to copy the configuration stored in Random Access Memory (RAM) to Non-Volatile Random Access Memory (NVRAM)?

A. router# copy running-config startup-config
B. router(config)# copy running-config startup-config
C. router# copy startup-config running-config
D. router(config)# copy startup-config running-config

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The router# copy running-config startup-config command is used to copy the configuration stored in Random Access Memory (RAM) to Non-Volatile Random Access Memory (NVRAM). This command is issued inprivileged EXEC mode. The syntax of the command is as follows:

router# copy running-config startup-config

The parts of the command are as follows:

- running-config is the running configuration stored in RAM.
- startup-config is the startup configuration stored in Non-Volatile Random Access Memory (NVRAM).

The router(config)# copy running-config startup-config command is incorrect because the copy run start command (abbreviated) is not issued in global configuration mode. It is executed in privileged EXEC mode.

The router# copy startup-config running-config command is incorrect because this command is used to copy the configuration stored in NVRAM to RAM.

The router(config)# copy startup-config running-config command is incorrect because neither the copy run start nor the copy start run commands are executed in global configuration mode. Moreover, the copy startup-config running-config command is used to copy the configuration stored in NVRAM to RAM.

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

References:

https://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/mgx_8850/software/mgx_r3/rpm/rpm_r1-1/configuration/guide/appc.html#wp1002710

QUESTION 115
What is the possible IP range that can be assigned to hosts on a subnet that includes the address 192.168.144.34/29?

A. 192.168.144.32 - 192.168.144.63
B. 192.168.144.33 - 192.168.144.38
C. 192.168.144.33 - 192.168.144.48
D. 192.168.144.28 - 192.168.144.40

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Range 192.168.144.33 - 192.168.144.38 is the correct answer. To determine the range of addresses that can be assigned in a subnet, you must first determine the network ID of the subnetwork and the broadcast address of the subnetwork. All addresses that can be assigned to hosts will lie between these endpoints. The network ID can be obtained by determining the interval between subnet IDs. With a 29-bit mask, the decimal equivalent of the mask will be 255.255.255.248. The interval between subnets can be derived by subtracting the value of the last octet of the mask from 256. In this case, that operation would be 256 - 248 = 8. Therefore, the interval is 8.

The first network ID will always be the classful network you started with (in this case 192.168.144.0). Each subnetwork ID will fall at 8-bit intervals as follows:

192.168.114.0
192.168.144.8
192.168.144.16
192.168.144.24
192.168.144.32
192.168.144.40

We can stop at the 192.168.144.40 address because the address given in the scenario, 192.168.144.34, is in the network with a subnet ID of 192.168.144.32. Therefore, since the broadcast address for this network will be 1 less than the next subnet ID (192.168.144.39), the valid range of IP addresses is 192.168.144.33 - 192.168.144.38. 192.168.144.39 will be the broadcast address for the next subnet, and 192.168.144.40 will be the first valid address in the next subnet.

None of the other answers is the correct range.

Objective:
Network Fundamentals

Sub-Objective:
Apply troubleshooting methodologies to resolve problems

References:

https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html#ustand_ip_add