200-301

Number: 200-301
Passing Score: 800
Time Limit: 120 min
File Version: 1

200-301

Exam A

QUESTION 1
You are the network administrator for your company and have configured Cisco Discovery Protocol (CDP) in your network. You recently noticed that when devices send large numbers of CDP neighbor announcements, some devices are crashing. You decide to disable CDP on the router.

Which command should you use to achieve the objective?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
You should use the no cdp run command to disable CDP on the router. Due to a known vulnerability regarding the handling of CDP by Cisco routers and switches when devices send large numbers of CDP neighbor announcements, some devices can crash or cause abnormal system behavior. To overcome this problem, you can disable CDP for the entire router by using the no cdp run command.

You cannot use the set cdp disable command to disable CDP on the router. This command disables CDP on an entire Catalyst switch.
You cannot use the no cdp enable command to disable CDP on the router. This command disables CDP on a specific interface.
You cannot use the no cdp advertise-v2 command to disable CDP on the router. This command disables CDPv2 advertisements.

Objective:

LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Support > Using Cisco Discovery Protocol

Cisco > Support > Technology Support > Network Management > Cisco's Response to the CDP Issue > Document ID: 13621

QUESTION 2
Which of the following protocols allow the root switch location to be optimized per VLAN? (Choose all that apply.)

A. PVST+
B. RSTP
C. PVRST
D. STP

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Both Per VLAN Spanning Tree Plus (PVST+) and Per VLAN Rapid Spanning Tree (PVRST) protocols allow for a spanning tree instance for each VLAN, allowing for the location optimization of the root bridge for each VLAN. These are Cisco proprietary enhancements to the 802.1d and 802.1w standards, respectively.

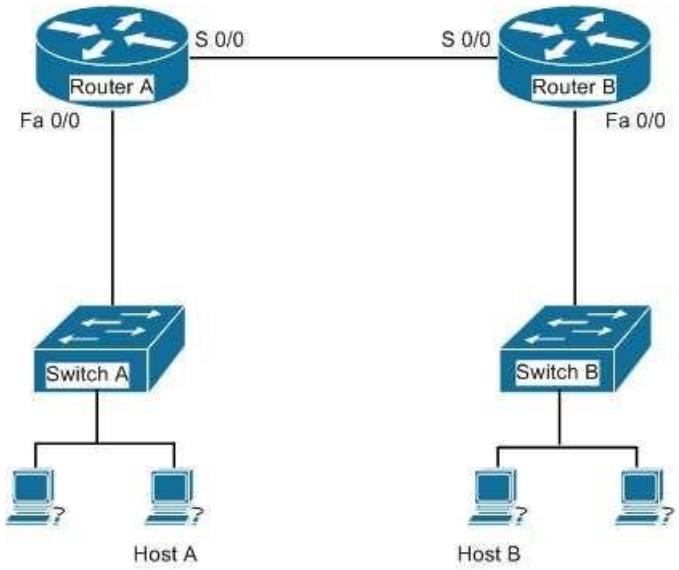
Rapid Spanning Tree Protocol (RSTP) is another name for the 802.1w standard. It supports only one instance of spanning tree.

Spanning Tree Protocol (STP) is another name for the 802.1d standard. It supports only one instance of spanning tree.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Cisco Home > Support > Technology Support > LAN Switching

QUESTION 3
Your assistant just finished configuring a small test network as part of his training. The network is configured as shown in the diagram below:



When testing the configuration, you find that Host A in the diagram cannot ping Host B.

Which of the following pairs of connections are required to be in the same subnet for Host A to be able to ping Host B? (Choose all that apply.)

A. The IP address of Host A and the IP address of the Fa0/0 interface of Router A
B. The IP address of the Fa0/0 interface of Router A and the IP address of the Fa0/0 interface of Router B
C. The IP address of Host A and the IP address of the Fa0/0 interface of Router B
D. The IP address of Host A and the IP address of Switch A
E. The IP address of the S 0/0 interface of Router A and the IP address of the S 0/0 interface of Router B
F. The IP address of Host A and the IP address of Host B
G. The IP address of Host B and the IP address of the Fa0/0 interface of Router B

Correct Answer: AEG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following pairs of connections are required to be in the same subnet:

- the IP address of Host A and the IP address of the Fa0/0 interface of Router A

- the IP address of the S 0/0 interface of Router A and the IP address of the S 0/0 interface of Router B
- the IP address of Host B and the IP address of the Fa0/0 interface of Router B

When troubleshooting a correctly labeled network diagram for IP addressing problems, one must start on one end and trace each link in one direction, ensuring at each step that the interfaces are in the same subnet. A switch simply passes the packet to the router; therefore, the IP address of the switch is not important. It performs its job even if it has no IP address.

Moving from Host A to Host B, however, the following links must be in the same subnet:
- The IP address of Host A and the IP address of the Fa0/0 interface of Router A
- The IP address of the S0/0 interface of Router A and the IP address of the S0/0 interface of Router B -
The IP address of Host B and the IP address of the Fa0/0 interface of Router B

Neither of the switch addresses is important to the process.

If all other routing issues are correct, it is also not required for Host A and Host B to be in the same subnet.

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

References:
Cisco > Home > Support > Technology Support > IP > IP Routing > Design > Design Technotes > IP Addressing and Subnetting for New Users

QUESTION 4
Which two fields are present in the output of the show ip interface brief command? (Choose two.)

A. YES?
B. Helper address
C. OK?
D. Method
E. Proxy ARP

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Sample output of the show ip interface brief command is as follows:

```
Router# show ip interface brief
Interface IP-Address OK? Method Status Protocol
Ethernet0 10.108.00.5 YES NVRAM up up
Ethernet1 unassigned YES unset administratively down down
Loopback0 10.108.200.5 YES NVRAM up up
Serial0 10.108.100.5 YES NVRAM up up
Serial1 10.108.40.5 YES NVRAM up up
Serial2 10.108.100.5 YES manual up up
Serial3 unassigned YES unset administratively down down
```

The following fields are present in the output of the show ip interface brief command:

OK?: If the value of this field is "yes", it represents that the IP address is valid. If the value of this field is "No", it represents an invalid IP address.
Method: This field can have one of the following values:
▪ RARP or SLARP: Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request ▪
BOOTP: Bootstrap protocol
▪ TFTP: Configuration file obtained from TFTP server
▪ Manual: Manually changed by CLI command
▪ NVRAM: Configuration file in NVRAM
▪ IPCP: ip address negotiated command
▪ DHCP: ip address dhcp command ▪
unassigned: No IP address ▪ unset:
Unset ▪ other: Unknown
▪ Interface: Refers to the type of interface.
▪ IP-Address: Refers to the IP address assigned to the interface.

Status: Displays the interface status. Possible values in this field are as follows:
▪ up: Interface is administratively up.
▪ down: Interface is down. ▪ administratively down:
Interface is administratively down.

Protocol: An indicator of the operational status of the routing protocol for this interface.

YES? is not a valid field in the output of the show ip interface brief command.

Helper address and Proxy ARP fields are present in the output of the show ip interface command, not the show ip interface brief command.

Objective:
Network Fundamentals Sub-
Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:
Cisco > Cisco IOS IP Addressing Command Reference > show ip interface

QUESTION 5
Which two modes are Cisco Internetwork Operating System (IOS) operating modes? (Choose two.)

A. User Privileged mode
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:
Network Fundamentals Sub-
Objective:
Select the appropriate cabling type based on implementation requirements

References:
Cisco Documentation > RPM Installation and Configuration > IOS and Configuration Basics > Cisco IOS Modes of Operation

QUESTION 6
Which of the following accurately describes the purpose of a trunk?

A. A trunk is used to carry traffic for a single VLAN and is typically used between switches.
B. A trunk is used to carry traffic for a single VLAN and is typically used between a switch and an end-user device.
C. A trunk is used to carry multiple VLANs and is typically used between switches.
D. A trunk is used to carry multiple VLANs and is typically used between a switch and a server.

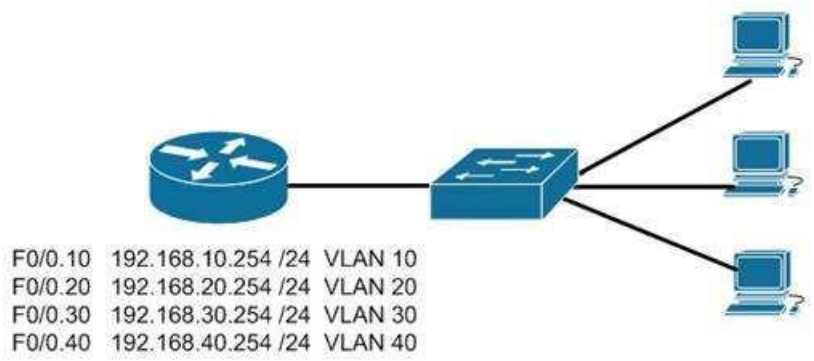
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Trunk links are used between switches to allow communications between hosts that are in the same VLAN, but connected to different switches. Trunk links do not allow hosts in different VLANs to communicate, unless there is an additional trunk link connecting to a Layer 3 device, such as a router or a multilayer switch. Trunk links do allow a host in VLAN 10 on SwitchA to communicate with a host in VLAN 10 on SwitchB. Similarly, a host in VLAN 20 on SwitchA could also communicate with a host in VLAN 20 on SwitchB. A trunk link supports all VLANs by default, and frames that are not traveling on the native VLAN are "tagged" with the VLAN ID of the originating port before being sent over the trunk. The receiving switch reads the VLAN ID and forwards the frame to the appropriate host in the same VLAN.

The other options are incorrect because trunk links do not carry data for a single VLAN, nor are trunks used between switches and hosts (such as workstations and servers).

When a trunk link is extended to a router for the purpose of enabling routing between VLANs, the physical connection that the link connects to is usually subdivided logically into subinterfaces. Then each subinterface is given an IP address from the same subnet as the computers that reside on that VLAN. Finally, each computer in the VLAN will use the corresponding IP address on the matching subinterface of the router as its default gateway. In the example below, the switch has five

VLANs created and some hosts connected to it. If hosts from different VLANs need to communicate, the link between the router and the switch must be a trunk link.



Furthermore, the physical link on the router must be subdivided into subinterfaces and addressed according to the legend shown for each subinterface in the diagram. For example, the configuration for VLAN 10 shown in the diagram would be as follows:

Router(config)# interface f0/0.10
Router(config-if)#encapsulation dot1q 10
Router(config-if)#ip address 192.168.10.254 255.255.255.0

Finally, each computer in VLAN 10 should have its default gateway set to 192.168.10.254.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Describe and verify switching concepts

References:

QUESTION 7
What will be the effects of executing the following set of commands? (Choose all that apply.)

```
router(config)# router eigrp 44 router
(config-router)# network 10.0.0.0 router
(config-router)# network 192.168.5.0
```

A. EIGRP will be enabled in AS 44
B. EIGRP instance number 44 will be enabled
C. EIGRP will be activated on the router interface 10.0.0.2/8

D. EIGRP will be activated on the router interface 192.168.5.9/24 E. EIGRP will be activated on the router interface 10.0.5.8/16
F. EIGRP will be activated on the router interface 192.168.6.1/24

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The effects of executing this set of commands will be that Enhanced Interior Gateway Routing Protocol (EIGRP) will be enabled in Autonomous System (AS) 44 and will be active on the router interfaces 10.0.0.2/8,192.168.5.9/24, and 10.0.5.8/16.

The router eigrp 10 command is used to enable EIGRP on a router. The network 10.0.0.0 and network 192.168.5.0 commands are used to activate EIGRP over any interfaces that fall within the major networks 10.0.0.0 and 192.168.5.0, or within any subnets of these classful networks. The network commands in EIGRP configuration ignore any subnet-specific information by default. Since the IP address 10.0.5.8.9/24 is in a subnet of the Class A IP network 10.0.0.0, and only the first octet (byte) of a Class A IP address represents the major (classful) network, the remaining bytes are ignored by the network command.

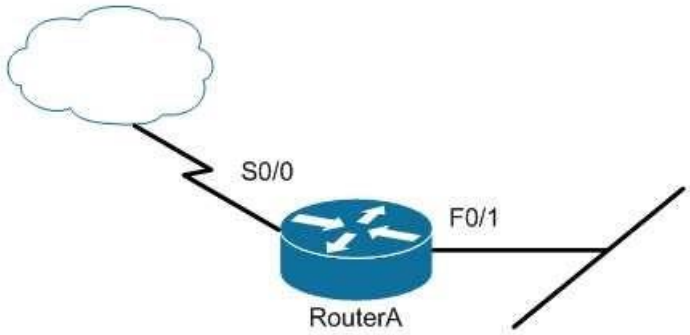
EIGRP instance number 44 will not be enabled. The number 44 in the command does not represent an instance of EIGRP; it represents an autonomous system (AS) number. The autonomous-system parameter of the router eigrp command (router eigrp 44) specifies the autonomous system number. To ensure that all the routers in a network can communicate with each other, you should specify the same autonomous system number on all routers.

EIGRP will not be activated on the router interface 192.168.6.1/24. This interface does not exist within the Class C network 192.198.5.0 or Class A network 10.0.0.0, or within any of their subnets.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > Cisco IOS Software > Configuring EIGRP > Enabling EIGRP
CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 10: EIGRP, pp. 389-390.

QUESTION 8
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 shutdown command 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 encapsulation type 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 not be 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:
Cisco > Support > Administrative Commands > shutdown

QUESTION 9
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?

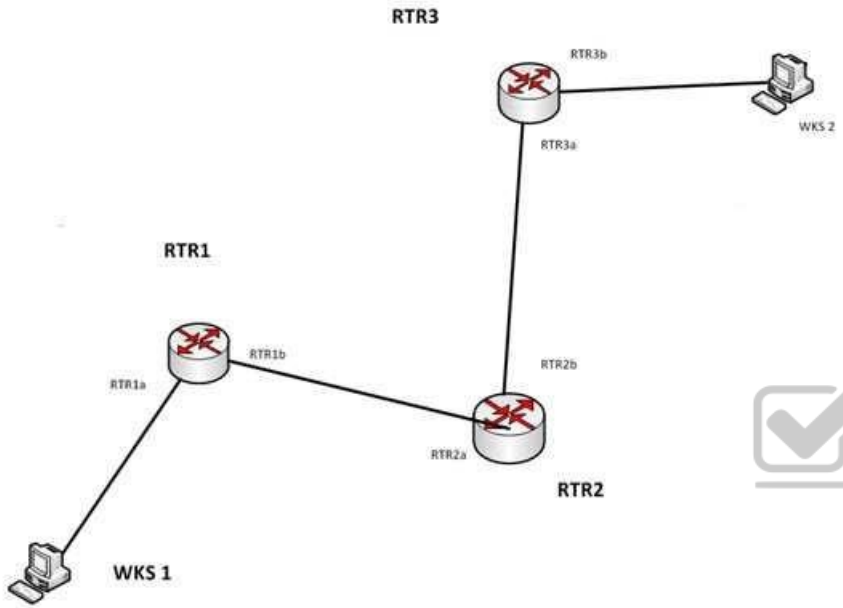
A. Source IP address
B. Destination MAC address
C. Source port number
D. Destination IP address

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 to RTR3a	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:
MAC address changes for every new network

QUESTION 10
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:
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 Link layer. 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
Entry address(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 CDPv2 advertisements 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 Management Sub-
Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:
Cisco > Cisco IOS Network Management Command Reference > schema through show event manager session cli username > show cdp neighbors detail

QUESTION 11
Your assistant is interested in gathering statistics about connection-oriented operations.

Which of the following should be done to enhance the accuracy of the information gathered?

A. configure an IP SLA responder on the destination device
B. configure an IP SLA responder on the source device
C. schedule the operation on the destination device
D. add the verify-data command to the configuration of the operation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Any IP SLA operations accuracy can be enhanced by configure an IP SLA responder on the destination device. It is important to note that only Cisco devices support the configuration as a responder.

You do not configure an IP SLA responder on the source device. You schedule the operation on the source device and the destination device is the one that is configured as a responder.

You do not schedule the operation on the destination device. You schedule the operation on the source device and the destination device is the one that is configured as a responder.

Adding the verify-data command to the configuration of the operation will not enhance the accuracy of the information gathered. When data verification is enabled, each operation response is checked for corruption. Use the verify-data command with caution during normal operations because it generates unnecessary overhead.

Objective:

Infrastructure Management Sub-
Objective:
Troubleshoot network connectivity issues using ICMP echo-based IP SLA

References:
IP SLAs Configuration Guide, Cisco IOS Release 15M > Configuring IP SLAs TCP Connect Operations

QUESTION 12
You are the network administrator for your company. You have installed a new router in your network. You want to establish a remote connection from your computer to the new router so it can be configured. You are not concerned about security during the remote connection.

Which Cisco IOS command should you use to accomplish the task?

A. ssh
B. telnet
C. terminal
D. virtual

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The telnet command should be used to establish a remote connection from your computer to the router. The syntax of the command is as follows:

telnet {{hostname | IP_address mask interface_name} | {IPv6_address interface_name} | {timeoutnumber}}

The following parameters are used with the telnet command:
hostname: Specifies the name of the host.
interface_name: Specifies the name of the network interface to which you need to telnet.
IP_address: Specifies the IP address of the host.
IPv6_address: Specifies the IPv6 address associated to the host. timeout number:
Specifies the number of minutes that a telnet session can be idle.

The following features are the key characteristics of Telnet:
- It is a client server protocol.
- It uses TCP port number 23.
- It is used to establish a remote connection over the internet or Local Area Network (LAN).

- Telnet does not encrypt any data sent over the connection; that is, the data travels in clear text.
- A Cisco router supports five simultaneous telnet sessions, by default. These lines are called vty 0-4.
- A successful Telnet connection requires that the destination device be configured to support Telnet connections, which means it must be configured with a Telnet password.
- The telnet command can also be used to test application layer connectivity to a device.

The ssh command is incorrect because this command is used to remotely establish a secure connection between two computers over the network.

The terminal command is incorrect because this command is used to change console terminal settings.

The virtual command is incorrect because this command is used along with the http and telnet parameters to configure a virtual server.

Objective:
Infrastructure Management Sub-
Objective:
Configure and verify device management

References:
Cisco > Cisco IOS Terminal Services Command Reference > telnet

QUESTION 13
You are configuring a WAN connection between two offices. You cannot ping between the routers in a test. The Serial0 interface on RouterA is connected to the Serial1 interface on RouterB.

The commands you have executed are shown below. What is the problem with the configuration?

```
RouterA(config)#username RouterB password lie
RouterA(config)#interface serial0
RouterA(config-if)#encapsulation ppp
RouterA(config-if)#ppp authentication chap

RouterB(config)#username RouterA password lie
RouterB(config)#interface serial0
RouterB(config-if)#encapsulation ppp
RouterB(config-if)#ppp authentication chap
```

A. The passwords are incorrectly configured
B. The usernames are incorrectly configured
C. The wrong interface has been configured
D. The encapsulation is incorrect on RouterA
E. The encapsulation is incorrect on RouterB

F. The authentication types do not match

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:
The two routers are connected using Serial0 on RouterA and Serial1 on RouterB. However, the configuration commands were executed on interface Serial0 on RouterB. So although the configuration itself is completely correct, it is configured on the wrong interface.

The passwords are correct. The passwords should match on both routers. In this case, they are both set to lie. If even one character does not match, including character casing, the authentication and the connection will fail.

The usernames are correct. The username should be set to the host name of the peer router. In this case, RouterA's username is set to RouterB and RouterB's username is set to RouterA, which is correct.

The encapsulations are correct. They are both set to PPP, which is the correct type of encapsulation when using authentication.

The authentication types do match. They are both set to CHAP. It is possible to configure two authentication methods, with the second used as a fallback method in cases where the other router does not support the first type. The command below would be used to enable CHAP with PAP as a fallback method:

```
RouterB(config-if)#ppp authentication chap pap
```


Objective: WAN
Technologies Sub-
Objective:
Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:
Cisco > Home > Support > Technology Support > WAN > Point-To-Point Protocol (PPP) > Design > Design Technotes > Understanding and Configuring PPP CHAP Authentication

QUESTION 14
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/extended range) spanning multiple switches

References:
Cisco > Support > LAN Switching > Virtual LANS / VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Configuring VLAN Trunk Protocol (VTP) > Document ID: 98154

QUESTION 15
You are discovering that there are differences between the configuration of EIGRP for IPv6 and EIGRP for IPv4. Which statement is true with regard to the difference?

A. A router ID is required for both versions
B. A router ID must be configured under the routing process for EIGRP for IPv4
C. AS numbers are not required in EIGRP for IPv6

D. AS numbers are not required in EIGRP for IPv4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Both versions of EIGRP require a router ID. The difference is that with EIGRP for IPv6, you must configure a router ID under the routing process if there are no IPv4 addresses on the router. In EIGRP for IPv4, the router can select one of the configured IPv4 addresses as the router ID.

A router ID can be configured under the routing process for EIGRP for IPv4, but it is not required. In EIGRP for IPv4, the router can select one of the configured Pv4 addresses as the router ID.

AS numbers are required in both versions of EIGRP.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Home > Articles > Cisco Certification > CCNA Routing and Switching > C > Cisco ICND2 Foundation Learning Guide: Implementing an EIGRP Solution > Implementing EIGRP for IPv6

QUESTION 16
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 1 ip address
  192.168.20.244 255.255.255.240 no
  shutdown exit ip default-gateway
  192.168.20.241
line vty 0 15
password cisco login exit
```

B.
```
interface fastethernet 0/1 ip address
  192.168.20.244 255.255.255.240 no
```

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

```
  line vty 0 15 login exit
```
D. `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
```

E. `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
```
F. `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
```

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

The following command set is correct:

```
interface vlan 1

ip address 192.168.20.244 255.255.255.240

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 the IP 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 to a 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-gateway
192.168.20.241

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

ip address 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-bit mask 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 Management Sub-
Objective:
Configure and verify device management

References:
Home>Support>Product Support>End-of-Sale and End-of-life Products>Cisco Catalyst 6000 Series Switches>Troubleshoot and Alerts> Troubleshooting TechNotes>Configuring a Management IP Address on Catalyst 4500/4000, 5500/5000, 6500/6000, and Catalyst Fixed Configuration Switches

QUESTION 17
What command should you use to quickly view the HSRP state of the switch for all HSRP groups of which the switch is a member?

A. switch# show standby brief
B. switch# show ip interface brief
C. switch# show hsrp
D. switch# show standby

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The command show standby brief should be used to quickly view the HSRP state of a switch for all HSRP groups of which it is a member. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address.

The command show standby can be used to display detailed information about HSRP groups of which a switch is a member. This command would not provide a quick view. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch.

The command show ip interface brief is useful in that lists the interfaces and displays the basic IP configuration of each. This output would include the IP address of the interface and the state of the interface, but not HSRP information.

The command show hsrp is not a valid command due to incorrect syntax.

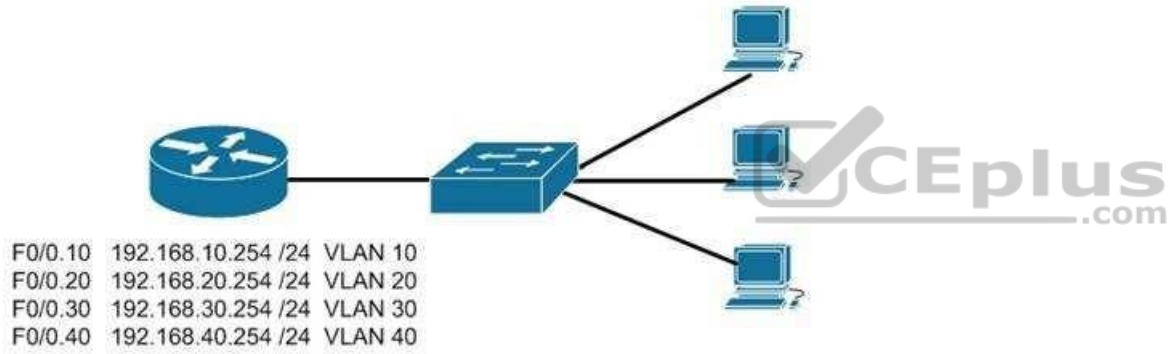
Objective:
Infrastructure Services Sub-
Objective:
Configure, verify, and troubleshoot basic HSRP

References:
Cisco > Cisco IOS IP Application Services Command Reference > show standby
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 18
You are connecting a new computer to Switch55. The new computer should be placed in the Accounting VLAN. You execute the show vlan command and get the following output:

```
Switch55#show vlan
VLAN Name Status Ports
1 default active Fa0/1, Fa0/2, Fa0/3,
Fa0/7, Fa0/8, Fa0/9,
Fa0/14, Fa0/16, Fa0/23,
Fa0/19, Fa0/20, Fa0/23
10 sales active Fa0/10, Fa0/22
20 accounting active Fa0/5, Fa0/6, Fa0/15
30 hr active Fa0/11, Fa0/12
40 it active Fa0/17
<<output omitted>>
```

Examine the additional network diagram.



What action should you take to place the new computer in the Accounting VLAN and allow for inter-VLAN routing?

A. Connect the new computer to Fa0/1
B. Connect the new computer to Fa0/14
C. Connect the new computer to Fa0/5
D. Configure a dynamic routing protocol on the router interface

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

Explanation:
Switchport Fa0/5 can be used to place the computer in the Accounting VLAN.

The diagram indicates that a router has been configured as a "router-on-a-stick" to perform inter-VLAN routing between VLANs 10, 20, 30 and 40. The show vlan output indicates that interfaces Fa0/5, Fa0/15, and Fa0/6 have been assigned to VLAN 20, the Accounting VLAN:

```
20 accounting active Fa0/5, Fa0/6, Fa0/15
```

Switchports Fa0/1 and Fa0/14 are both in the default VLAN, as indicated by the portion of the output describing the switch ports that are unassigned and therefore still residing in the default VLAN:

```
1 default active Fa0/1, Fa0/2, Fa0/3,
Fa0/7, Fa0/8, Fa0/9,
Fa0/14, Fa0/16, Fa0/23,
Fa0/19, Fa0/20, Fa0/23
```

It is not necessary to configure a dynamic routing protocol on the router. Since the router is directly connected to all four subinterfaces and their associated networks, the networks will automatically be in the router's routing table, making inter-VLAN routing possible.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco > Support > Cisco IOS LAN Switching Command Reference > show vlan
Cisco Networking Essentials 2nd Edition, by Troy McMillan (ISBN 1119092159). Sybex, 2015. Chapter 15: Configuring Inter-VLAN Routing

QUESTION 19
What two devices can be connected to a router WAN serial interface that can provide clocking? (Choose two.)

A. CSU/DSU
B. switch
C. modem
D. hub

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A router DTE interface must receive a clock rate from the DCE end and the rate can be provided by either a CSU/DSU or a modem. Therefore, the connection between the local router and the service provider can be successfully completed by adding either of these devices between the service provider and the local router.

Switches and hubs are neither capable of providing the clock rate nor able to complete the connection between the local router and the service provider.

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

References:
Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies

QUESTION 20
Which Cisco Internetwork Operating System (IOS) command is used to view the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets that are sent and received?

A. show eigrp neighbors
B. show ip eigrp interfaces
C. show ip eigrp packets
D. show ip eigrp traffic
E. show ip route
F. show ip eigrp topology

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show ip eigrp traffic command is used to view the number of EIGRP packets that are sent and received. The syntax of the command is:

Router# show ip eigrp traffic [autonomous-system-number]

The autonomous-system-number parameter is optional. The output of the command is as follows:

```
Router# show ip eigrp traffic

IP-EIGRP Traffic Statistics for process 78
Hellos sent/received: 2180/2005
Updates sent/received: 70/21
Queries sent/received: 3/1
Replies sent/received: 0/3
Acks sent/received: 22/11
```

The show ip eigrp neighbors command is incorrect because it does not show the number of packets sent or received. It does show IP addresses of the devices with which the router has established an adjacency, as well as the retransmit interval and the queue count for each neighbor, as shown below:

```
Router# show ip eigrp neighbors
IP-EIGRP Neighbors for process 49
Address Interface Holdtime Uptime Q Seq SRTT RTO
(secs) (h:m:s) Count Num (ms) (ms)
146.89.81.28 Ethernet1 13 0:00:41 0 11 4 20
146.89.80.28 Ethernet0 12 0:02:01 0 10 12 24
146.89.80.31 Ethernet0 11 0:02:02 0 4 5 20
```

The show ip eigrp interfaces command is incorrect because this command is used to view information about the interfaces configured for EIGRP.

The show ip eigrp packets command is incorrect because it is not a valid Cisco IOS commands.

The show ip route command will not display EIGRP packets that are sent and received. It is used to view the routing table. When connectivity problems occur between subnets, this is the logical first command to execute. Routers must have routes to successfully send packets to remote subnets. Using this command is especially relevant when the underlying physical connection to the remote network has been verified as functional, but routing is still not occurring.

The show ip eigrp topology command is incorrect because it does not show the number of packets sent or received. This command displays all successor and feasible successor routes (if they exist) to each network. If you are interested in that information for only a specific destination network, you can specify that as shown in the output below. When you do, the command output displays all possible routes, including those that are not feasible successors:

```
Router# show ip eigrp topology 25.0.0.5 255.255.255.255

IP-EIGRP topology entry for 25.0.0.5/32 State is Passive, Query
origin flag is 1, 1 Successor(s), FD is 41152000

<output omitted>

10.1.0.1 (serial0), from 10.1.0.1 composite
metric is 46152000/41640000
<output omitted>
10.0.0.2 (serial0.1), from 10.0.0.2
composite metric is 53973240/120256
<output omitted>
10.1.0.3 (serial0), from 10.1.0.3
composite metric is 46866176/46354176
<output omitted>
10.1.1.1 (serial0.1), from 10.1.1.1
composite metric is 46670776/46251776
<output omitted>
```

In the above output, four routers are providing a route to the network specified in the command. However, only one of the submitted routes satisfies the feasibility test. This test dictates that to be a feasible successor, the advertised distance of the route must be less than the feasible distance of the current successor route.

The current successor route has a FD of 41152000, as shown in the first section of the output. In the values listed for each of the four submitted routes, the first number is the feasible distance and the second is the advertised distance. Only the route received from 10.0.0.2 (second section) with FD/AD values of 53973240/120256 satisfies this requirement, and thus this route is the only feasible successor route present in the topology table for the network specified in the command.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Cisco IOS IP Routing Protocols Command Reference > Routing Information Protocol Commands > show ip eigrp traffic

QUESTION 21
Which statement is NOT true regarding Internet Control Message Protocol (ICMP)?

A. ICMP can identify network problems.
B. ICMP is documented in RFC 792.

C. ICMP provides reliable transmission of data in an Internet Protocol (IP) environment.

D. An ICMP echo-request message is generated by the ping command.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ICMP does NOT provide reliable transmission of data in an Internet Protocol (IP) environment. The Transmission Control Protocol (TCP) is used to provide reliable transmission of data in an IP environment.

The following statements are TRUE regarding ICMP:

- ICMP can identify network problems.
- ICMP is documented in RFC 792.
- An ICMP echo-request message is generated by the ping command.
- An ICMP echo-reply message is an indicator that the destination node is reachable.
- ICMP is a network-layer protocol that uses message packets for error reporting and informational messages.

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast TCP and UDP protocols

References:
Cisco > Internetworking Technology Handbook > Internet Protocols (IP) > Internet Control Message Protocol (ICMP)

QUESTION 22
What is the valid host address range for the subnet 172.25.4.0 /23?

A. 172.25.4.1 to 172.25.5.254
B. 172.25.4.10 to 172.25.5.210
C. 172.25.4.35 to 172.25.5.64
D. 172.25.4.21 to 172.25.5.56

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

For the subnet 172.25.4.0, the valid host range will start at 172.25.4.1 and end at 172.25.5.254.

To determine the valid range of addresses in a subnet, one must determine the subnet number or network ID and the broadcast address of the subnet and all valid addresses will lie within those boundaries.

In this case:
Network address: 172.25.0.0
Subnet mask in decimal: 255.255.254.0 (/23 indicates 23 bit in the mask)
Subnet mask in binary: 11111111.11111111.11111110.00000000

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

In this scenario:
Number of subnet bits: 7 (the binary 1s in the third octet of the subnet mask)
Number of subnets: 27 = 128
Number of host bits: 9 (the binary 0s in the subnet mask)
Number of hosts: 29 - 2 = 510

These formulas are useful when determining if a subnet mask/network ID combination will support a given number of hosts.

To determine the boundaries of each of the 128 subnets that this mask will yield, you should utilize a concept called the interval or block size. This number helps to identify the distance between network IDs. Determining the network IDs allows the identification of the broadcast address for each subnet, because the broadcast address for any particular subnet will always be the last address before the next network ID. The interval is determined by the value of the far right-hand bit in the mask, which is 2 in this case. Then it is applied to the octet where the mask ends. In this case, the first 4 network IDs are:

172.25.0.0
172.25.2.0
172.25.4.0
172.25.6.0
...incrementing by two at each point

Therefore, the valid addresses in the 172.25.4.0 network are framed by the two addresses that cannot be used: 172.25.4.0 (network ID) and 172.25.5.255 (broadcast address, or the last address before the next network ID). The addresses within these boundaries are 172.25.4.1 to 172.25.5.254.

For subnet 172.25.0.0, the valid host range will run from 172.25.0.1 to 172.25.1.254. The broadcast address for subnet 172.25.0.0 will be 172.25.1.255.

For subnet 172.25.2.0, the valid host range will run from 172.25.2.1 to 172.25.3.254. The broadcast address for subnet 172.25.2.0 is 172.25.3.255.

For the subnet 172.25.4.0, the valid host range will run from 172.25.4.1 to 172.25.5.254. The broadcast address for subnet 172.25.4.0 is 172.25.5.255.

Always remember that the first address of each subnet is the network ID, and as such cannot be used as a host or router IP address. Also, the last address of each subnet is the broadcast address for the subnet, and as such cannot be used as a host or router IP address.

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast IPv4 address types

References:
Cisco > Support > Technology Support > IP > IP Routing > Design > Design Technotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

QUESTION 23
Which of the following are port roles in the Rapid Spanning Tree Protocol (RSTP)? (Choose three.)

A. Alternate
B. Listening
C. Routing
D. Designated
E. Backup
F. Blocking
G. Discarding

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are five port roles in RSTP:

- Root port: the closest port to the root bridge in terms of path cost. There can be only one root port on each switch, and the root switch is the only switch in the network that does not have a root port.
- Designated port: a forwarding port to the root bridge. All versions of STP require each network segment to have only one path toward the root bridge, to avoid bridging loops in redundantly connected environments. All bridges connected to a given segment listen to one another's BPDUs and agree that the bridge that is sending the best BPDU is the designated bridge for the segment.
- Alternate port: a blocking port that becomes the root port if the active root port fails.
- Backup port: a blocking port that becomes the designated port if an existing designated port fails.
- Disabled port: a disabled port has no role within the operation of spanning tree.
- RSTP was designed to provide rapid convergence of the spanning tree in case of changes to the active topology, such as switch failure.

RSTP has the following similarities to STP:
- RSTP elects the root switch using the same parameters as STP.

- RSTP elects the root port using the same rules as STP.
- Designated ports on each LAN segment are elected in RSTP in the same way as STP.

Listening is a port state, not a port role. Listening is the STP transitional state while a port is preparing to enter a root or designated role.

Blocking is a port state, not a port role. A blocking port is inactive in STP spanning tree, and blocking is not a port state in RSTP. In RSTP that port state is called discarding.

The routing port does not exist in the RSTP topology.

Discarding is an RSTP port state, not a port role.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Support > Technology Support > LAN Switching > Spanning Tree Protocol > Troubleshoot and Alerts > Troubleshooting TechNotes > Understanding Rapid Spanning Tree Protocol (802.1w)

QUESTION 24
Which of the following cables would be used to connect a router to a switch?

A. v.35
B. crossover
C. rollover

D. straight-through

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A straight-through cable would be used. When connecting "unlike" devices, such as a switch to a router, a straight-through cable is used. This is a cable where the wires are in the same sequence at both ends of the cable.

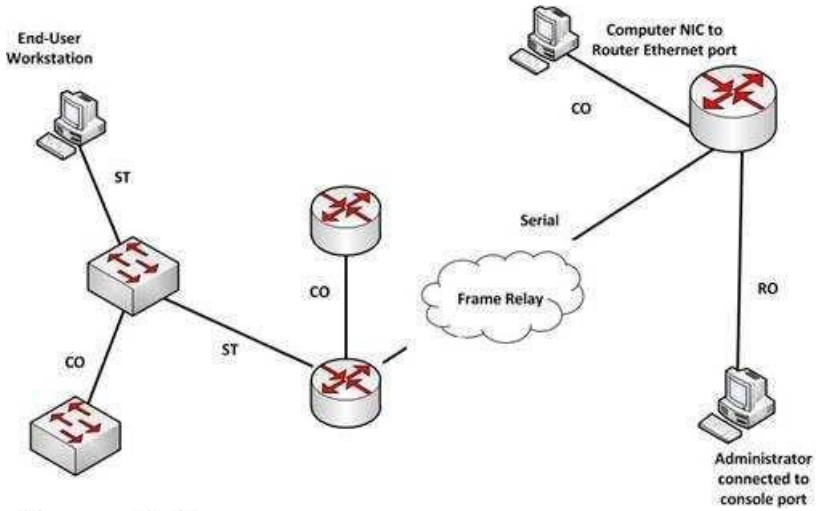
NOTE: The one exception to this general rule of connecting unlike devices with a straight-through cable is when a computer NIC is connected to an Ethernet port on a router. In that case, a crossover cable is used.

A v.35 cable is used to connect serial connections between routers. This cable has a male DB-60 connector on the Cisco end and a male Winchester connector on the network end. It comes in two types: DCE and DTE. It is often used to simulate a WAN connection in lab environments. In that case, the DCE end acts as the CSU/DSU and is the end where the clock rate is set. A CSU/DSU (Channel Service Unit/Data Service Unit) is a device that connects the router to the T1 or T3 line.

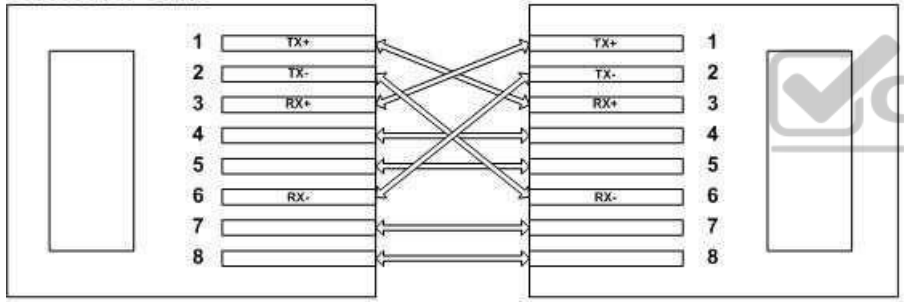
A crossover cable has two wires reversed and is used to connect "like" devices, such as a switch to a switch. It is also used when a computer NIC is connected to an Ethernet port on a router.

A rollover cable is used to connect to the console port of a router to configure the router. It is also called a console cable.

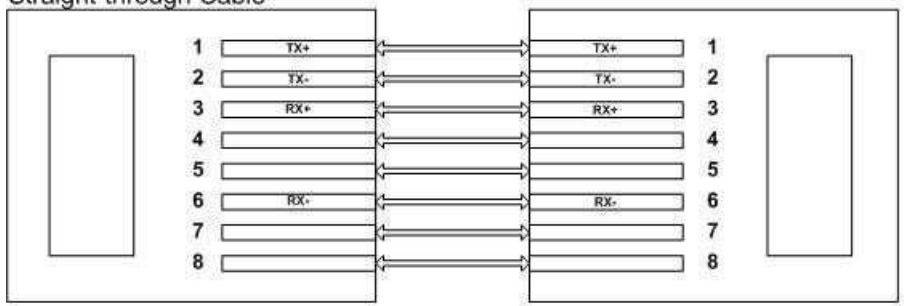
The diagram below illustrates the correct usage of each of the cable types shown using the following legend: ▪
SO Ethernet Straight through Cable
▪ CO Ethernet Crossover Cable
▪ Serial Serial cable
▪ RO Rollover cable



Crossover Cable



Straight-through Cable



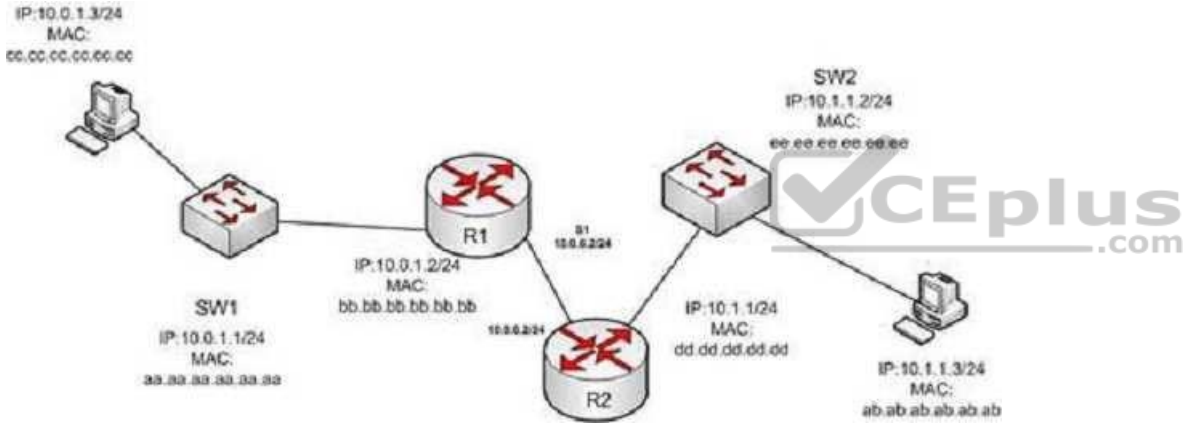
RX = Receive, TX = Transmit

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

References:
Cisco > Product Support > Routers > Cisco 1000 Series Routers > 5-in-1 V.35 Assembly and Pinouts > Document ID: 46803

Cisco > Tech Notes > Cabling Guide for Console and AUX Ports > Document ID: 12223

QUESTION 25
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.ddD. 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 arrives at 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:
Cisco > IOS Technology Handbook > Routing Basics

QUESTION 26
Which two security features can be configured to prevent unauthorized access into the network through a networking device? (Choose two.)

A. Anti-Replay
B. Traffic filtering
C. Authentication
D. IPSec network security

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Traffic filtering and authentication security can be configured to prevent unauthorized access into the network through a networking device. Unauthorized access to the company's network should be blocked because unauthorized access can damage a company's network. Attackers may access confidential data, plant a virus in the network, or flood the network with illegitimate packets. Therefore, preventive measures should be taken to block any unauthorized access.

The traffic filtering security feature uses two measures to prevent unauthorized access into the network: access lists and Cisco IOS firewalls.

Access lists are configured to determine which traffic to block and which traffic should be forwarded at the router interfaces. The following types of access lists are available when using Cisco devices:
- Basic access lists: Allow only specific traffic through the device; other traffic is dropped.

▪ Extended access lists: Used to filter the traffic based on source IP address, destination IP address, port numbers, or protocols.

Cisco IOS firewalls provide various security features according to your needs. Following are the key components of Cisco IOS firewall:
▪ Context-based Access Control (CBAC): Filters TCP and UDP packets on the basis of application layer protocol session information.
▪ Cisco IOS firewall Intrusion Detection System (IDS): Used to detect suspicious activity. IDS are used to watch packets and sessions as they flow through the router and scan then to match IDS signatures. If the packet is detected as suspicious, the packet is dropped. ▪ Authentication Proxy: Used to apply specific security policies on a per-user basis.

Authentication security can be used to prevent unauthorized access to the network. When a user attempts to access a service or host within the network, they must enter credentials such as their user name and password. If the credentials are correct, then access is provided; otherwise, the user is not allowed to access the service.

Anti-replay and IPSec network security cannot prevent unauthorized access through a networking device into the network. Anti-replay prevents the capture and replay of packets on a network. Although a good security feature to deploy it does not specifically address access to the network through a device. IPSec is used to encrypt and protect the integrity of data that travels through the network, not control access through a device.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Tech Notes > Cisco Guide to Harden Cisco IOS Devices > Document ID: 13608

QUESTION 27
Which Cisco IOS command is used on a Cisco Catalyst 6500 series switch to view the spanning-tree protocol (STP) information for a virtual LAN (VLAN)?

A. show spanning tree
B. show spanning-tree vlan
C. show spantree
D. show spantree vlan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show spanning-tree vlan Cisco IOS command is used on a Catalyst 6500 series switch to view the spanning-tree information for a VLAN, such as information on the root switch (bridge ID, root path, root cost), as well as local switch.

The following is sample output of the show spanning-treevlan vlan-id command:

```
Switch# show spanning-tree vlan 1
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 000c.00d3.5124
Cost 19
Port 2 (FastEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000c.14f5.b5c0
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

The show spanning tree command is incorrect because it is not the correct syntax of a Cisco IOS command.

The show spantree and show spantree vlan commands are incorrect because these are CatOS commands, not Cisco IOS commands.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Cisco IOS LAN Switching Command Reference > show spanning-tree

QUESTION 28
Which Enhanced Interior Gateway Routing Protocol (EIGRP) packet type is used for neighbor discovery?

A. Hello
B. Update
C. Queries
D. Replies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Hello packets are used for neighbor discovery. These are sent as multicasts and do not require an acknowledgement.

Update packets are sent to communicate the routes used by a router to converge. When a new route is discovered or the convergence process is completed, updates are sent as multicast. During topology table synchronization, updates are sent as unicasts to neighboring peers.

Query packets are sent when a router performs route computation and cannot find a feasible successor. These packets are sent to neighboring peers asking if they have a feasible successor to the destination network.

Reply packets are sent in response of a query packet. These are unicast and sent to the originator of the query.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

QUESTION 29
Which layer in the Open Systems Interconnection (OSI) model enables coding and conversion functions for application layer data?

A. Presentation layer
B. Session layer
C. Application layer
D. Physical layer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Presentation layer in the OSI model enables coding and conversion functions for application layer data. Data formatting and encryption is done at this layer. The Presentation layer converts data into a format that can be accepted by the application layer. The Presentation layer is also known as the syntax layer, which provides translation between different data formats by using a common format.

The Session layer in the OSI model does not enable coding and conversion functions for the application layer data. It is used to create, manage, and terminate sessions between communicating nodes. The session layer handles the service requests and service responses that take place between different applications.

The Application layer in the OSI model does not enable coding and conversion functions for the application layer data. The application layer is responsible for interacting directly with the application, and provides application services, such as e-mail and File Transfer Protocol (FTP).

The Physical layer in the OSI model does not enable coding and conversion functions. The Physical layer consists of the hardware that sends and receives data on a carrier. The protocols that work at the Physical layer include Fast Ethernet, RS-232, and Asynchronous Transfer Mode (ATM). The Physical layer is the base layer in the OSI model.

The three remaining layers in the OSI model are the Transport, Network, and Data Link layers. The Transport layer is 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).

The Network layer is used to define the network address or the Internet Protocol (IP) address that is then used by the routers to forward the packets. The Data Link layer ensures reliable transmission of data across a network.

The seven layers of the OSI model are sequentially interconnected to each other. From the top to the bottom, the seven layers are:
Layer 7: Application
Layer 6: Presentation
Layer 5: Session
Layer 4: Transport
Layer 3: Network
Layer 2: Data Link
Layer 1: Physical

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

References:
Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems

QUESTION 30
Below is the output of the show ip route command from one of your routers:

```
R66#show ip route
.....
1.0.0.0/30 is subnetted, 4 subnets
C   1.1.1.0 is directly connected, FastEthernet0/1
O   1.1.1.4 [110/2] via 1.1.1.2, 00:10:04, FastEthernet0/1
O   1.1.1.8 [110/2] via 1.1.1.13, 00:10:04, FastEthernet0/0
C   1.1.1.12 is directly connected, FastEthernet0/0
172.16.0.0/24 is subnetted, 4 subnets
C   172.16.0.0 is directly connected, Ethernet0/0/0
O   172.16.1.0 [110/11] via 1.1.1.2, 00:10:04, FastEthernet0/1
O   172.16.2.0 [110/12] via 1.1.1.13, 00:09:24, FastEthernet0/0
          [110/12] via 1.1.1.2, 00:09:24, FastEthernet0/1
O   172.16.3.0 [110/11] via 1.1.1.13, 00:10:04, FastEthernet0/0
```

What does the value 110 represent in the output?

A. OSPF administrative distance
B. EIGRP administrative distance
C. OSPF cost
D. EIGRP cost

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The value of 110 represents the administrative distance of the route, which in this case was learned by OSPF. OSPF routes are always indicated by an O to the left of the route details. The two values in brackets in each route entry indicate the administrative distance on the left of the forward slash. The value to the right of the slash is the cost of the route. Therefore, [110/2] represents an administrative distance of 110 and a cost of 2.

The value of 110 does not represent EIGRP administrative distance because the route was not learned from EIGRP. If it were, the route would have a D to the left of the route details. Moreover, the default administrative distance of EIGRP is 90, not 110.

The values do not represent OSPF cost. The cost value is on the right side of the forward slash within the brackets in each route entry. For example, the route entry O 1.1.1.4 [110/2] via 1.1.1.2, 00:10:04, FastEthernet0/1 indicates an OSPF cost of 2.

The values do not represent an EIGRP cost. First, if it were an EIGRP route, the route would have a D to the left of the route details. Moreover, the cost value is located within the square brackets to the right of the forward slash in each route entry. The only cost values shown in the table are 2, 11, and 12.

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

References:
Cisco > Support > Cisco IOS IP Routing: Protocol-Independent Command Reference > show ip route
The Anatomy of "Show IP Route"

QUESTION 31
With the following equipment list, which of the following network scenarios could be supported?

- Two IP subnets of 255.255.255.0
- Seven 48-port switches
- Two router interfaces

A. 300 workstations in a single broadcast domain, each workstation in its own collision domain
B. 300 workstations, with 150 workstations in two broadcast domains and each workstation in its own collision domain
C. 300 workstations, with 150 workstations in two broadcast domains and all workstations in the same collision domain
D. 600 workstations, with 300 workstations in two broadcast domains and each workstation in its own collision domain

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This equipment will support 300 workstations, with 150 workstations divided in two broadcast domains and each workstation in its own collision domain. Subnets with a 24-bit mask (255.255.255.0) yield 254 addresses in each network, so 150 is within those limits. Also, seven 48-port switches make 336 ports available. After subtracting out 2 ports per switch for connecting the switches to each other and the router (a total of 14) that leaves 321 ports yielding 160 for each subnet (with one left over) . Two subnets require two router interfaces, which are available in the scenario, and since switches are in use, each switch port is its own collision domain.

This equipment will not support 300 workstations in a single broadcast domain with each workstation in its own collision domain. With a 24-bit mask, 300 workstations cannot be placed in a single subnet.

This equipment will not support 300 workstations, 150 each in two broadcast domains and all workstations in the same collision domain. The 300 workstations cannot be placed in the same collision domain when using switches. If hubs were in use that would be possible, but not desirable.

This equipment will not support 600 workstations, 300 each in two broadcast domains; each workstation in its own collision domain. 600 workstations cannot be placed in two subnets when using the mask 255.255.255.0. Each subnet can only hold 254 workstations, not 300. Moreover, 300 workstations cannot be placed in the same collision domain when using switches. If hubs were in use that would be possible but not desirable.

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

References:
Cisco Documentation > Internetwork Design Guide > Internetworking Basics

QUESTION 32
Which of the following is NOT a true statement regarding Virtual Private Networks (VPNs)?

A. A VPN is a method of securing private data over public networks
B. IPsec is a method for providing security over VPN
C. Frame Relay is a Layer 3 VPN technology
D. IPsec provides packet-level encryption
E. A Cisco VPN solution provides increased security, reduced cost, and scalability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Frame Relay is a Layer 2 VPN technology, providing connectivity over switched carrier Wide Area Networks (WANs). Packets are encapsulated in Frame Relay frames, and assigned Data Link Connection Identifiers (DLCIs) to identify to the local Frame Relay switch the virtual circuit (VC) that the data should follow.

A VPN is a method of securing private data over public networks (such as the Internet), so this is a true statement.

IPsec is a security framework that provides security for data traveling over VPNs, so this is a true statement. It is an open standard protocol framework that is used to secure end-to-end communications.

IPsec allows for encryption at the packet level (Layer 3) when configured in tunnel mode, so this is a true statement.

VPN solutions such as those supported by Cisco ASA firewalls and Cisco integrated routers provide the following benefits:▪
Lower desktop support costs
▪ Threat protection
▪ Flexible and cost-effective licensing

▪ Reduced cost and management complexity

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco > Internetworking Technology Handbook > Frame Relay
Cisco > Internetworking Technology Handbook > Virtual Private Networks (VPNs)

QUESTION 33
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:
Cisco > Cisco IOS IPv6 Command Reference > ipv6 host

QUESTION 34
Which two statements are TRUE of synchronous serial ports? (Choose two.)

A. These ports can be used to provide leased-line or dial-up communications.
B. These ports do not support the High-Level Data Link Control (HDLC) encapsulation method.
C. An AUI connector is used with serial ports.
D. These ports can be used to configure high-speed lines (E1 or T1).
E. An RJ-45 connector is used with serial ports.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Synchronous serial ports can be used to provide leased-line or dial-up communications, and these ports can be used to configure high-speed lines (E1 or T1). The following are also true of synchronous serial ports:
▪ With the help of synchronous serial lines, dialers can be configured, which are then used to support dial-on-demand routing. ▪
These ports are found on several serial network interface processors and cards.

The option stating that synchronous serial ports cannot support High-Level Data Link Control (HDLC) encapsulation method is incorrect because HDLC is the default encapsulation method configured on serial interfaces.

The option stating that an AUI connector is used with serial ports is incorrect because AUI is a connector used with Ethernet ports.

The option stating that an RJ-45 connector is used with serial ports is incorrect because RJ-45 and RJ-48 connectors are used with ISDN BRI connections.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:

QUESTION 35
Refer to the following sample output:

```
*: interface is up
IHQ: pkts in input hold queue IQD: pkts dropped from input queue
OHQ: pkts in output hold queue OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec) RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec) TXPS: tx rate (pkts/sec)
TRTL: throttle count
Interface IHQ IQD OHQ OQD RXBS RXPS TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0 0 0 0 0 0 0 0 0 0
Serial0/0 0 0 0 0 0 0 0 0
FastEthernet0/1 0 0 0 0 0 0 0 0 0
Serial0/1 0 0 0 0 0 0 0 0
```

Which Cisco Internetwork Operating System (IOS) command produces this output?

A. show interfaces
B. show interfaces summary
C. show interfaces serial fast-ethernet
D. show interfaces fast-ethernet 0/0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show interfaces summary command will produce the given output. This command provides a summarized view of all interfaces configured on a device.

The show interfaces command is incorrect because this command does not produce the displayed output. This command is used to view information regarding statistics for specific interfaces. Without specifying an interface, a section for each interface will display, as in the example below for FastEthernet0:

```
FastEthernet0 is up, line protocol is down
Hardware is Fast Ethernet, address is 0019.e818.a3dd (bia
0019.e818.a3dd)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
--More
```


The show interfaces serial fast-ethernet command is incorrect because this is not a valid Cisco IOS command.

The show interfaces fast-ethernet 0/0 command is incorrect. Although it produces similar output, that output only relates to the FastEthernet 0/0 interface. An example of this output follows:

```
FastEthernet0 is up, line protocol is up
Hardware is Fast Ethernet, address is 0019.e818.a3dd (bia
0019.e818.a3dd)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops:105
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 1530000 bits/sec, 201 packets/sec
5 minute output rate 673000 bits/sec, 173 packets/sec
404737363 packets input, 23875417953 bytes, 11 no buffer
Received 1206930011 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
401877661 packets output, 23875417953 bytes, 0 underruns
0 output errors, 576297 collisions, 0 interface resets
0 babbles, 0 late collision, 2174225 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```


Notice that the line of output that says FastEthernet0 is up, line protocol is up indicates that Layers 1 to 3 of the OSI Model are functioning correctly. Also, in the lower portion, there are no values in the error counters such as input errors, output errors, and so on. Finally, make note in line 8 where the interface is set to autosense both the duplex and the speed. Duplex and speed must be in agreement between the NIC on the host and the switch port.

Objective:
Routing Fundamentals Sub-
Objective:
Troubleshoot basic Layer 3 end-to-end connectivity issues

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > show interfaces summary

QUESTION 36
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/extended range) spanning multiple switches

References:
Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25) > Understanding and Configuring VLANs, VTP, and VMPS

QUESTION 37
Which of the following commands will enable a global IPv6 address based on the Modified EUI-64 format interface ID?

A. ipv6 address 5000::2222:1/64
B. ipv6 address autoconfig
C. ipv6 address 2001:db8:2222:7272::72/64 link-local
D. ipv6 enable

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To configure the interface to create a global IPv6 address based on the Modified EUI-64 format interface ID, you must enable stateless autoconfiguration. In stateless autoconfiguration, the interface will receive the network prefix from the router advertisement (RA) and generate a full IPv6 address by spreading the 48-bit MAC address of the interface across 64 bits to complete the address. This can all be done simply by executing the ipv6 address autoconfig command at the interface configuration prompt.

The command ipv6 address 5000::2222:1/64 is used to manually assign a full IPv6 address to the interface without using stateless autoconfiguration or the eui-64 keyword to manually specify the first 64 bits and allow the last 64 bits to be generated from the MAC address of the interface.

The command ipv6 address 2001:db8:2222:7272::72/64 link local is used to configure a link-local address manually without allowing the system to generate one from the MAC address, which is the default method.

The command ipv6 enable is used to allow the system to generate a link-local address from the MAC address. Because this is the default behavior, the command is not required if any other ipv6 commands have been issued. Regardless of how many manual IPv6 addresses you configure, a link local address is always generated by default.

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

References:
Cisco > Product Support > Security > Cisco ASA 5500-X Series Firewalls > Configure > Configuration Guides > Cisco Security Appliance Command Line Configuration Guide, Version 7.2 > Chapter: Configuring IPv6 > Enforcing the Use of Modified EUI-64 Interface IDs in IPv6 Addresses Cisco > Support > Cisco IOS IPv6 Command Reference > ipv6 address

QUESTION 38
Which of the following commands is used to verify the link-local, global unicast, and multicast addresses of an IPv6 router?

A. show ipv6 neighbors (only link-local addresses)
B. show ipv6 route
C. show ipv6 protocols
D. show ipv6 interface

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:
The show ipv6 interface command is used to verify the link-local, global unicast, and multicast addresses assigned to an IPv6-enabled router interface. The show ipv6 interface command displays information regarding that interface, such as the physical state, MTU, and IPv6 enable/disable state.

Here is the partial output of the show ipv6 interface command on an IPv6-enabled router named rtrA:

```
rtrA# show ipv6 interface FastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is
FE80::6339:7BFF:FE5D:A031/64
Global unicast address(es):
2001:7067:90D1:1::1, subnet is 2001:7067:90D1:1/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF5D:A031
MTU is 1500 bytes
<output omitted>
```


In the sample output, you can see that the Fa0/1 interface of rtrA has the link-local address FE80::6339:7BFF:FE5D:A031/64 and the global unicast address 2001:7067:90D1:1::1. The global unicast address is not in EUI-64 format because when the ipv6 address command was issued, the eui64 keyword was not used. If the EUI-64 format had been specified with the eui64 keyword, the global unicast address would have been 2001:7067:90D1:1:6339:7BFF:FE5D:A031.

An IPv6-enabled interface has not only a link-local and global unicast address, but also one or more multicast addresses. A multicast address is an IPv6 address that has the prefix FF00::/8. These addresses are assigned to interfaces of different nodes such that they appear as a logical group. This implies that when a packet is destined for a multicast address, that packet is delivered to all the interfaces that have the same multicast address. The various multicast groups are as follows:

- FF02::1 Indicates the group of all the nodes on the local segment
- FF02::2 Indicates the group of all the routers on the local segment
- FF02::1:FF00:0/104 Indicates a solicited-node multicast group for every unicast or anycast address assigned to the interface

You can also notice in the sample output that the Fa0/1 interface belongs to three multicast groups: FF02::1, FF02::2, and FF02::1:FF5D:A031. The first two multicast groups refer to the all-host and all-router multicast groups, respectively. The third group, FF02::1:FF5D:A031, is the solicited-node multicast address. This

address is created for every unicast or anycast address. A solicited-node multicast address is determined by assigning the least significant 24 bits of the unicast address to the least significant 24 bits of the FF02::1:FF00:0 address.

The show ipv6 neighbors command displays the link-local /global unicast addresses of the neighbors, including other information such as state and the next-hop interface.

The show ipv6 route command is used to view the IPv6 routing table on the router. This command displays the prefixes, administrative distance, metric, and nexthop addresses for various IPv6 networks.

The show ipv6 protocols command is used to view the active routing protocols for IPv6 on the router. This command shows the interfaces, redistribution status, and summarization status about each of the routing protocols enabled on the router.

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

References:
Cisco IOS IPv6 Command Reference > show ipv6 eigrp topology through show ipv6 nat statistics > show ipv6 interface
Cisco IOS IPv6 Command Reference > show ipv6 nat translations through show ipv6 protocols > show ipv6 neighbors
Cisco IOS IPv6 Command Reference > show ipv6 nat translations through show ipv6 protocols > show ipv6 protocols
Cisco > Products & Services > Cisco IOS and NX-OS Software > Cisco IOS Technologies > IPv6 > Product Literature > White Papers > Cisco IOS IPv6 Multicast Introduction
Cisco > IPv6 Implementation Guide, Release 15.2M&T > Implementing IPv6 Multicast

QUESTION 39
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-41 is 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:
Cisco Documentation > Internetwork Design Guide > Designing Switched LAN Internetworks > Technologies for Building Switched LAN Internetworks
Cisco > Troubleshooting Technotes > Cisco 7000 Series Routers > Cabling Guide for Console and AUX Ports > Types of RJ-45 Cabling

QUESTION 40
A router is running a classful routing protocol. Which command will enable this router to select a default route when routing to an unknown subnet of a network for which it knows the major network?

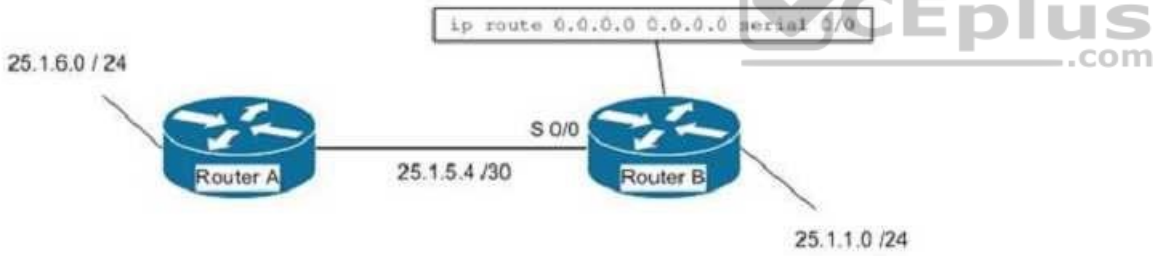
A. ip classless
B. no ip classless

C. auto-summary
D. no auto-summary

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The ip classless command causes a routing protocol to change its default behavior of discarding any traffic that is bound for unknown subnets of a known classful network. If the command is enabled, the router tries to match the most number of bits possible against the route in its routing table. Alternatively, the router will use the default route rather than dropping the packet.

For an example of this behavior, examine the diagram below. The ip route 0.0.0.0 0.0.0.0 serial 0/0 command has been issued on Router B. If the 25.1.6.0/24 network is unknown to Router B, then under normal circumstances, Router B would NOT use its configured default route. Instead, it would drop any packets addressed to that unknown network, because when a router knows a route to a major classful network or its subnets (in this case, 25.1.5.0/30 and 25.1.1.0/24), it will not use a statically configured default route to forward traffic to an unknown subnet of that network (in this case 25.1.6.0/24). In the scenario described in the diagram, Router B will drop the packet. However, if the ip classless command has been executed, it will use the default route and send the traffic to Router A.



The ip classless command is a global configuration mode command enabled by default in Cisco IOS version 12.0 and later. If the default route is learned from IS-IS or OSPF, as opposed to being statically configured as in the above example, the ip classless command is not necessary for the router to use the default route.

The no ip classless command on routers will disable the forwarding of packets destined to an unknown subnet of a known classful network. Therefore, it is an incorrect option.

The auto-summary command is used to allow automatic summarization of subnet routes into network-level routes. This is a command executed in router configuration mode.

Classless routing protocols such as Routing Information Protocol version 2 (RIPv2) and Enhanced Interior Gateway Routing Protocol (EIGRP) perform automatic route summarization at classful boundaries. The no auto-summary command is used to turn off this route summarization.

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

References:
Cisco > Articles > Cisco Certification > CCNP > CCNP Self-Study: Advanced IP Addressing

Cisco > Cisco IOS IP Addressing Services Command Reference > IP Addressing Commands > ip classless

QUESTION 41
Which Cisco IOS command is used to configure encapsulation for a PPP serial link on a Cisco router?

A. encapsulation ppp
B. encapsulation ip ppp
C. ip encapsulation ppp
D. encapsulation ppp-synch

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
PPP is a Layer 2 protocol encasulation type that supports both synchronous and asynchronous circuits and provides built-in security mechanaims. The encapsulation ppp interface configuration mode command is used to configure encapsulation for a PPP (Point to Point Protocol) serial link on a Cisco router. PPP

encapsulation provides for router-to-router and host-to-network connections over both synchronous and asynchronous circuits. Serial links are configured to use Cisco High Level Data Link Control (HDLC) encapsulation, by default, on Cisco routers. The Cisco version of HDLC is incompatible with the industry standard version used on other router brands because it contains a type field that identifies the underlying network protocol being encapsulated by HDLC. This is a beneficial feature of Cisco HDLC but makes it incompatible with other router brands.

For this reason, a Cisco router that is going to be connected to a non-Cisco router should be configured to use PPP instead of the default. The encapsulation ppp interface configuration mode command will do this. If you set one of the routers for PPP and leave the other router at the default encapsulation for a serial connection, the connection will fail due to incompatible encapsulation.

You would use the show run command to verify matching encapsulation types. In the partial output of the show run command for two routers shown below, it can be seen that although one of the routers has the encapsulation ppp command in its configuration, the other does not. The absense of the encapsulation ppp command means that the default HDLC is being used. This incompatibility will cause both routers to report a serial interface up, line protocol down condition since the connection is live, but the Layer 2 framing is misconfigured.

```
router1#show run                    router2#show run
<output omitted>                    <output omitted>
interface serial 0/0               interface serial 0/1
encapsulation ppp
```

If authentication between the routers is also required, the authentication pap, authentication ms-chap, or authentication chap commands could be used to apply Password Authentication Protocol (PAP), Microsoft Challenge Authentication Protocol (MS-CHAP), or Challenge Authentication Protocol (CHAP) authentication to the connection, respectively.

A full configuration of a serial link for using PPP with authentication is as shown below:

```
Router1(config)#interface Serial0
Router1(config-if)#encapsulation ppp
Router1(config-if)#ppp authentication pap
```

Note above that the third line enables PAP authentication, which is not secure. Alternately, you can use CHAP authentication (which is secure) with the ppp authentication chap command. Regardless of which authentication mechanism you choose, these authentication commands will only be accepted on an interface where PPP encapsulation has been enabled, which rules out any non-serial interfaces.

The third type of encapsulation that can be configured on a serial WAN link is Frame Relay, which can be selected with the encapsulation frame relay command under the interface.

In summary, the three encapsulation types available for WAN serial links are PPP, HDLC, and Frame Relay. The command for each is as follows, executed under the interface configuration prompt:

encapsulation ppp
encapsulation hdlc
encapsulation frame relay

All other options are invalid commands.

Objective: WAN
Technologies Sub-
Objective:
Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

QUESTION 42
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 IP address 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:
PChuck's Network > Microsoft Windows Networking, Security, and Support > Reading IPConfig and Diagnosing Network Problems

QUESTION 43
Which of the following commands would instruct OSPF to advertise ONLY the 192.168.10.0/24 network in Area 0?

A. Router(config)# router ospf 1
Router(config-router)# network 192.168.10.0 0.0.0.255 area 0
B. Router(config)# router ospf 1
Router(config-router)# network 192.168.11.0 0.0.0.255 area 0
C. Router(config)# router ospf 1
Router(config-router)# network 192.168.10.0 255.255.255.0 area 0
D. Router(config)# router ospf 1
Router(config-router)# network 192.168.10.0 0.0.255.255 area 0

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command Router(config-router)# network 192.168.10.0 0.0.0.255 area 0 would instruct OSPF to advertise the 192.168.10.0 network in Area 0. It is executed in OSPF process 1 configuration mode, as indicated by the prompt Router(config-router)#. This command correctly states the network as 192.168.10.0 and uses the proper wildcard mask of 0.0.0.255.

The command Router(config-router)# network 192.168.11.0 0.0.0.255 area 0 is incorrect because it advertises the 192.168.11.0/24 network instead of the 192.168.10.0/24 network.

The command Router(config-router)# network 192.168.10.0 255.255.255.0 area 0 is incorrect because it uses a regular mask instead of a wildcard mask.

The wildcard mask in OSPF network statements must be expressed inversely, and not as a regular subnet mask. If the network you are configuring for OSPF operation is 192.168.10.0/24, then the inverse version of a /24 mask (or 255.255.255.0) would be 0.0.0.255. The correct command, Router(config-router)# network 192.168.10.0 0.0.0.255 area 0,will configure OSPF to run over any local interfaces assigned an IP address beginning with 192.168.10, since the inverse mask dictates that the first three octets must be a match.

The command Router(config-router)# network 192.168.10.0 0.0.255.255 area 0 is incorrect because it uses an improper wildcard mask. This mask would instruct OSPF to advertise any network with a prefix longer than the 192.168.0.0/16 network.

When routing does not seem to be working correctly, one of the first things to check is whether OSPF is operating on the proper interfaces. OSPF is enabled by network statements. To verify the network statements that were entered, you should execute the show run command and examine the output. If the network statement is configured so that the interface on the router is not in that network, OSPF will not operate on that interface. For example, suppose that Router A has an interface of 192.168.5.1/30 and the show run command produces the following output:


```
<output omitted> router
ospf 2 area 0 network
192.168.5.0 0.0.0.4
```

In this case, OSPF will not operate on the interface because the router interface is not in the network indicated by the network statement. The problem is not the network address but the wildcard mask. For a 30-bit mask, the wildcard should be 0.0.0.3, not 0.0.0.4. The wildcard mask can be determined by subtracting the regular mask value in the last octet (252) from 255, which is 3. The solution would to remove the incorrect statement and enter the correct statement as follows:

routerA(config)# router ospf 2 area 0
no network 192.168.5.0 0.0.0.4 area 0
network 192.168.5.0 0.0.0.3 area 0

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Cisco > Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T > Part 6: OSPF > Configuring OSPF > OSPF Configuration Task List > Enabling OSPF

QUESTION 44
You are the network administrator for your company. You have a Class B address range and are planning for a network that allows 150 hosts per subnet and at least 164 subnets.

Which subnet mask should you use to accomplish the task?

A. 255.255.192.0
B. 255.255.255.192C. 255.255.255.0
D. 255.255.255.252

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should use 255.255.255.0 as the subnet mask to allow 150 hosts per subnet and at least 164 subnets. The formulas used 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

Subnet mask in decimal: 255.255.255.0
Subnet mask in binary: 11111111.11111111.11111111.00000000
Number of subnet bits: 8 (binary 1s in the subnet octet of the subnet mask)
Number of host bits: 8 (binary 0s in the subnet mask)

In this scenario, we find that for 255.255.255.0:

Subnets that can be used: 28 = 256
Hosts that can be used: 28 - 2 = 254

The other options do not allow 150 hosts per subnet and at least 164 subnets.

If you use 255.255.192.0 as the subnet mask, then the total number of hosts that can be connected per subnet is 16382 (214 - 2 = 16382). However, there will be 4 subnets (22 = 4).

If you use 255.255.255.192 as the subnet mask, there will be 62 hosts (26 - 2 = 62).

If you use 255.255.255.252 as the subnet mask, there will be two hosts per subnet (22 - 2 = 2).

Note: This mask is frequently used for a subnet that connects two routers. In that case, there are two interfaces in the subnet, and thus it is most efficient use of the addressing space. This is also the most efficient way to address a point-to-point serial link.

A note about the formulas: You will always subtract 2 from the number of hosts (2number-of-host-bits - 2) because the all-zeroes bit address is reserved for the network address and the all-ones bit address is reserved for the broadcast address.

Before Cisco IOS Software Release 12.0, it was common practice to subtract 2 from the networks formula (2number-of-subnet-bits) to exclude 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 (2number-of-subnet-bits - 2) to calculate the number of valid subnets.

Objective:
Network Fundamentals Sub-
Objective:
Apply troubleshooting methodologies to resolve problems

References:
Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses
Cisco > Technology Support > IP > IP Addressing Services > Design TechNotes > Subnet Zero and the All-Ones Subnet > Document ID: 13711

QUESTION 45
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 of the 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, Port ID (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/extended range) spanning multiple switches

References:

QUESTION 46
Which Cisco command keeps unauthorized users from viewing passwords in the router configuration file?

A. enable secret
B. enable password
C. enable encryption

D. service encryption
E. service password-encryption

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The service password-encryption global configuration mode command keeps unauthorized users from viewing passwords in the router configuration file. The service password-encryption command encrypts all current and future passwords configured on the router, including the line password, virtual terminal password, console password, user name password, routing protocol passwords such as BGP neighbor passwords, the privileged command password, and authentication key passwords. Moreover, it encrypts any future passwords created on the router.

The encryption process occurs whenever the current configuration is built or a password is configured. The service password-encryption command will cause the router configuration file to display encrypted characters instead of passwords when the running-configuration or startup-configuration files are viewed.

The enable password command creates a password that will be required to enter privileged EXEC mode, but the password will not be encrypted.

The enable secret command provides encryption to the enable mode passwords but does not apply globally to all passwords configured on the router. It also does not encrypt any future passwords created on the router.

The enable encryption and service encryption commands are invalid.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Cisco IOS Security Command Reference > service password-encryption
Cisco Tech Notes > Cisco IOS Password Encryption Facts > Document ID: 107614

QUESTION 47
Which of the following statements are TRUE regarding carrier sense multiple access collision detection (CSMA/CD)? (Choose three.)

A. Networks are segmented into multiple collision domains using switches for CSMA/CD networks.
B. Networks are segmented into multiple broadcast domains using switches for CSMA/CD networks.
C. CSMA/CD networks normally operate on half-duplex mode.
D. CSMA/CD networks normally operate on full-duplex mode.
E. Gigabit Ethernet uses CSMA/CD as the media access control method.

F. Gigabit Ethernet uses carrier sense multiple access with collision avoidance (CSMA/CA) as the media access control method.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following statements are true:
- Networks are segmented into multiple collision domains using switches for CSMA/CD networks
- CSMA/CD networks normally operate on half-duplex mode
- Gigabit Ethernet uses CSMA/CD as its media access control method

CSMA/CD is a Local Area Network (LAN) access method used in Ethernet. In CSMA/CD, if a device or a node wants to send a packet in the network, it first determines if the network is free. If the network is not free, then the node will wait before sending the packet into a network. If the network is free, then the node sends the packet; if another device sends a packet simultaneously, their signals or packets collide. When the collision is detected, both packets wait for a random amount of time before retrying.

The option stating that networks are segmented into multiple broadcast domains using switches for CSMA/CD networks is incorrect because networks are segmented into multiple broadcast domains using routers for CSMA/CD networks.

The option stating that CSMA/CD networks normally operate on full-duplex mode is incorrect; these networks normally operate on half-duplex mode.

The option stating that gigabit Ethernet uses CSMA/CA as the media access control method is incorrect because gigabit Ethernet uses CSMA/CD as the media access control method.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Describe and verify switching concepts

References:

Cisco > Internetworking Technology Handbook > Introduction to LAN Protocols > LAN Media-Access Methods
Cisco > The Internet Protocol Journal - Volume 2, No. 3 > Gigabit Ethernet

QUESTION 48
Which of the following is a frame tagging method for identifying Virtual LAN (VLAN) memberships over trunk links?

A. STP
B. RIP
C. CDP

D. 802.1q

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
802.1q is a frame tagging method for identifying Virtual LAN (VLAN) memberships over trunk links. Frame tagging ensures identification of individual VLAN frames over a trunk link that carries frames for multiple VLANs. This frame tagging method is a standardized protocol developed by The Institute of Electrical and Electronics Engineers (IEEE). Cisco has also developed a proprietary frame tagging method, known as Inter-Switch Link (ISL).

When configuring a trunk link between a router and a switch, you must configure the physical interface on the router with one subinterface for each VLAN, and you must configure the physical ports on the router and the switch with the same encapsulation type, whether 802.1q or ISL.

Spanning Tree Protocol (STP) is not a frame tagging method, but a protocol used to remove switching loops in redundantly configured switched environments and create a single active Layer 2 path between any two network segments. Whenever a network segment can be handled by more than one switch, STP will elect one switch to take responsibility, and the other switches will be placed into a blocking state for the ports connected to that segment. In this way, only one switch receives and forwards data for this segment, removing the potential for generating multiple copies of the same frame. The benefits of STP include:

- Prevention of broadcast storms
- Prevention of multiple frame copies
- Media Access Control (MAC) address database stability

Routing Information Protocol (RIP) is not a frame tagging method, but a distance vector routing protocol. It populates routing tables dynamically about the topology changes.

Cisco Discovery Protocol is not a frame tagging method, but a Cisco proprietary protocol used to collect hardware and protocol information for directly connected Cisco devices. CDP has nothing to do with VLANs.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco > Support > Technology Support > LAN Switching > Layer-Three-Switching and Forwarding > Configure > Configuration Examples and Technotes > Configuring InterVLAN Routing and ISL/802.1Q Trunking on a Catalyst 2900XL/3500XL/2950 Switch Using an External Router

QUESTION 49
A packet is received with a destination IP address of 10.2.16.10.

```
Router# show ip route
<<output omitted>>

D 10.0.0.0 /8 [90/2172515] via 192.168.1.10, 00:00:44, Serial0/0
D 10.1.0.0 /16 [90/2144425] via 192.168.1.10, 00:01:03, Serial0/0
C 192.168.1.0 is directly connected, Serial0/0
C 192.168.4.0 is directly connected, Serial0/1
D 10.2.16.0 /24 [90/2162425] via 192.168.4.2, 00:00:25, Serial0/1
C 192.168.10.0 is directly connected, Serial1/0
D 10.2.32.0 /24 [90/2172425] via 192.168.10.254, 00:00:21, Serial1/0
          90/2172425] via 192.168.1.10, 00:03:33:, Serial0/1
```


What would the next hop IP address be for this packet?

A. 192.168.1.10
B. 192.168.4.2
C. 192.168.10.254
D. None; the packet will be dropped.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The packet will be routed to the next hop IP address of 192.168.4.2, since this routing table entry is the most specific match for the remote network. Packets are routed according to the most specific, or "longest," match in the routing table.

The packet in the scenario has a destination IP address of 10.2.16.10, which matches two entries in the routing table.

- 10.0.0.0 /8: this matches based on the /8 mask, where only the first byte has to match. The destination IP address of 10.2.16.10 has a first byte matching 10. If this were the only matching route table entry, it would be selected.
- 10.2.16.0 /24: The first 24 bits of this entry match the first 24 bits of the destination IP address of 10.2.16.10.

Therefore, the 10.2.16.0 /24 entry is selected for routing this packet because it most specifically matches the destination IP address, or has the longest number of matching bits.

The next hops of 192.168.1.10 and 192.168.10.254 will not be used, as these routes are not the most specific matches for the destination IP address of the packet.

It is interesting to note that packets that are destined for the 10.2.32.0 network will be load balanced across both serial 0/0 and serial 0/1 because the cost (2172425) is the same for both paths.

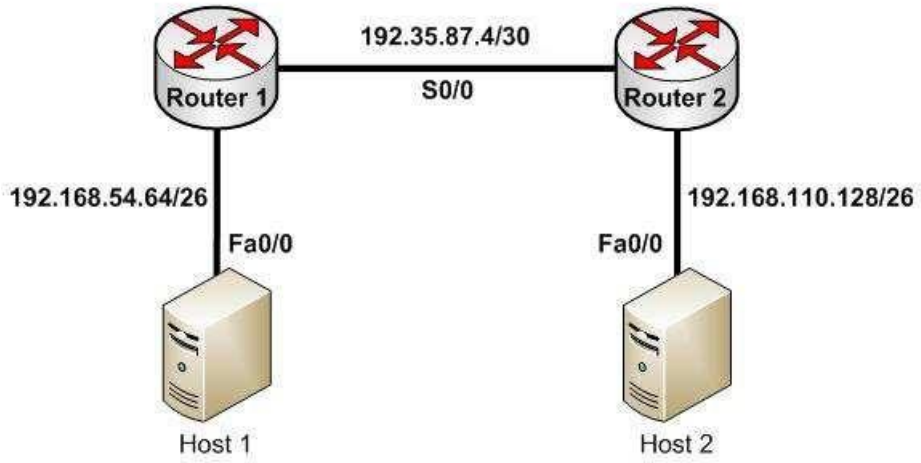
The packet will not be dropped because there is at least one routing table entry that matches the destination IP address of the packet.

To ensure that no packets are dropped, even if there is no matching route in the routing table, a default route could be configured as follows (next hop picked at random for illustration):

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

This configuration would instruct the router to send any packets that do match the existing routes to 192.168.1.1. For example, a packet destined for 201.50.6.8/24 would not match any routes in the table, and would thus be forwarded to 192.168.1.1.

If you understand how routing tables and routing advertisements work, it is relatively simple to describe the contents of a router's routing table without seeing the table directly. To do so, you would view the router's configuration and the configuration of its neighbors using show run, along with a diagram of its network connections. For example, examine the diagram of the two routers shown below along with their respective configurations:




```
hostname router 1          hostname router 2
router rip                              router rip
network 192.168.54.64                 network 192.168.110.128
ip route 0.0.0.0 0.0.0.0 192.35.87.5 <output omitted> <output omitted>
```

Based on this output and diagram, we can reconstruct the contents of the routing table for Router 1 as follows.

```
S*0.0.0.0/0 [1/0] via 192.35.87.5
R 192.168.110.128/26 [120/1] via 192.35.87.5 00:00:22, Serial 0/0
C 192.35.87.4/30 is directly connected, S0/0
C 192.168.54.64/26 is directly connected, Fa0/0
```

It will contain S*0.0.0.0/0 [1/0] via 192.35.87.5 because of the static default route indicated in line 4 of its configuration output.

It will contain R 192.168.110.128/26 [120/1] via 192.35.87.5 00:00:22, Serial 0/0 because Router 2 has a network 192.168.110.128 statement indicating that it will advertise this network to its neighbors.

It will contain the two routes C 192.35.87.4/30 is directly connected, S0/0 and C 192.168.54.64/26 is directly connected, Fa0/0 because all directly connected routes are automatically placed in the table.

Objective:
Routing Fundamentals Sub-
Objective:
Interpret the components of routing table

References:
Cisco > Support > IP > IP Routing > Design > Design TechNotes > Route Selection in Cisco Routers > Document ID: 8651

QUESTION 50
Which type of network connection requires a straight-through cable?

A. host to host
B. switch to router
C. switch to switch
D. host to router's Ethernet port

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A switch to router connection requires a straight-through cable. Straight-through cables are also used for host to switch communication.

A crossover cable is used to connect "like" devices, and a straight through cable is used when connecting "unlike" devices. The one exception to this rule is when connecting a computer NIC to an Ethernet port on a router, a crossover cable is used. In summary, the following list describes when to use crossover and straight through cables:

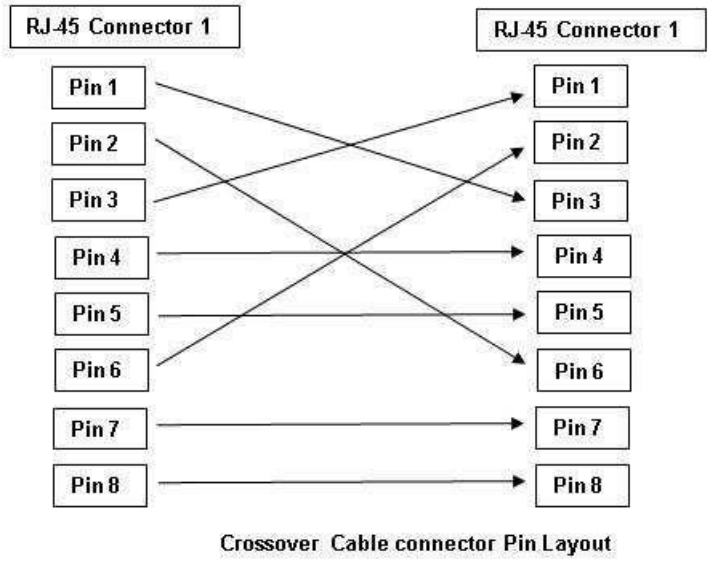
- Host to host Crossover
- Host NIC to router Crossover
- Host to switch Straight through
- Switch to Switch Crossover

- Switch to router Straight through

The difference between straight-through and crossover lies in the location of the wire termination on the two ends of an RJ-45 cable. If the unshielded twisted-pair (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 straightthrough.

On the other hand, if the Pin 1 of one side RJ-45 cable connected to Pin 3 of other end and Pin 2 connects to Pin 6 of other side, it is called as crossover cable. The cable type to be used depends upon circuit connection on the hardware. Some devices have ports that are capable of identifying the cable type and automatically adjusting the port setting to be a standard or uplink port.

Host-to-host, switch-to-switch, and host-to-Ethernet-port would all use a crossover cable to connect in the network. The following figure shows the pin layout for a crossover cable:



Crossover Cable connector Pin Layout

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

References:
Cisco > Product Support > End-of-Sale and End-of-Life Products > Cisco 7000 Series Routers > Troubleshooting Technotes > Cabling Guide for Console and AUX Ports > Document ID: 12223

QUESTION 51
Which of the following statements describes split horizon?

A. The router learns from its neighbor that a route has gone down, and the router sends an update back to the neighbor with an infinite metric to that route.
B. For a period of time, the router will ignore any route advertisements with a lower metric to a downed route.
C. A router will not send route information back out the same interface over which it was learned.
D. The moment a router determines a route has gone down, it will immediately send a route update with an infinite metric to that route.
E. The packets are flooded when a topology change occurs, causing network routers to update their topological databases and recalculate routes.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Split horizon is used to prevent routing loops in distance vector routing environments. It prevents a router from advertising a network back in the direction of the router from which it was learned. In this sense, route advertisements flow "downstream" (away from the route), but never "upstream" (back towards the advertised route).

Poison reverse describes when a router learns that a network has gone down, and the router sends an update back to the neighbor with an infinite metric.

Holddown describes when a router ignores any route advertisements that have a lower metric to a downed route.

Triggered updates describe when a router immediately sends a route update with an infinite metric, as opposed to waiting for its next regularly scheduled routing update.

Link State Advertisements (LSA) are packets that are flooded when a topology change occurs, causing network routers to update their topological databases and recalculate routes.

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast distance vector and link-state routing protocols

References:
Cisco > Articles > Network Technology > General Networking > Dynamic Routing Protocols

QUESTION 52
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 remote Data 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:
Cisco>Home>Support>Technology Support>IP>IP Routing>Technology Information>technology Whitepaper>EIGRP> Split Horizon and Poison Reverse

QUESTION 53
How is load balancing achieved when implementing HSRP?

A. By configuring multiple gateways on the routers
B. By using multiple HSRP groups

C. By configuring the same priority on all HSRP group members
D. By configuring multiple virtual router addresses

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When implementing Hot Standby Router Protocol (HSRP), load balancing is achieved by using multiple HSRP groups. Routers configured for HSRP can belong to multiple groups and multiple VLANs. By configuring one group to be active for Router A and standby for Router B, and the second group to be active for Router B and standby for Router A, both routers A and B can be used to pass traffic, as opposed to one sitting idle.

Load balancing cannot be achieved by configuring multiple gateways on the routers. The routers have one IP address. Each group will have a virtual IP address. In the configuration below, line 4 configures the virtual IP address, and is therefore the address that clients will use as their gateway:

```
interface fastethernet 0/1 no
switchport ip address 192.168.5.5
255.2555.255.0 standby 1 ip
192.168.5.10
```


Load balancing cannot be achieved by configuring the same priority on all HSRP group members. If that were done, one of the routers would become active and the others would remain inactive standbys. The active router will be the one with the highest IP address.

Load balancing cannot be achieved by configuring multiple virtual router addresses. Each HSRP group can only have one virtual address.

Objective:
Infrastructure Services Sub-
Objective:
Configure, verify, and troubleshoot basic HSRP

References:
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing

QUESTION 54

```
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 12.1.10.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

Which Cisco IOS command would produce the preceding menu-based prompt for additional information?

A. tracert 10.10.10.1
B. traceroute 12.1.10.2
C. ping 10.10.10.1
D. ping

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This menu-based prompt for additional information shown would be generated by the Cisco IOS ping command when issued without a target IP address. This is also known as issuing an extended ping. This command can be issued on the router to test connectivity between two remote routers. To execute an extended ping, enter the ping command from the privileged EXEC command line without specifying the target IP address. It takes the command into configuration mode, where various parameters, including the destination and target IP addresses, can be defined.

Note: You can only perform an extended ping at the privileged EXEC command line, while the normal ping works in both user EXEC mode and privileged EXEC mode.

The tracert command is incorrect because the tracert command is used by Microsoft Windows operating systems, not Cisco devices. This command cannot be run via the Cisco IOS command line interface. However, Microsoft's tracert utility is similar to Cisco's traceroute utility, which is to test the connectivity or "reachability" of a network device or host. The tracert command uses Internet Control Message Protocol (ICMP) to list all of the 'hops" or routers traversed to a destination.

The traceroute command is incorrect because this command uses Internet Control Message Protocol (ICMP) to list all of the 'hops" or routers traversed to a destination. It is also used to find routing loops or errors within a network.

The ping 10.10.10.1 command is incorrect because you when you issue this command you will either receive a reply from the destination or a destination unreachable message. It will not prompt for additional information as shown

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

References:
Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > ping
Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730 > The Extended ping Command
Cisco Documentation > Internetwork Troubleshooting Handbook > Troubleshooting TCP/IP

QUESTION 55
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 troubleshoot interswitch connectivity

References:

QUESTION 56
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:
Cisco Documentation > Internetworking Technology Handbook > Routing Basics

QUESTION 57
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 nat inside 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:

QUESTION 58
Which WAN switching technology is used by Asynchronous Transfer Mode (ATM)?

A. cell-switching
B. virtual switching
C. circuit-switching
D. packet switching

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Cell switching is used by Asynchronous Transfer Mode (ATM). ATM is an International Telecommunication Union-Telecommunications (ITU-T) standard for transmission of data, voice, or video traffic using a fixed size frame of 53 bytes, known as cells. Out of these 53 bytes, the initial five bytes are header information and the remaining 48 bytes are the payload.

The term virtual switching is incorrect because it is not a valid WAN switching technology.

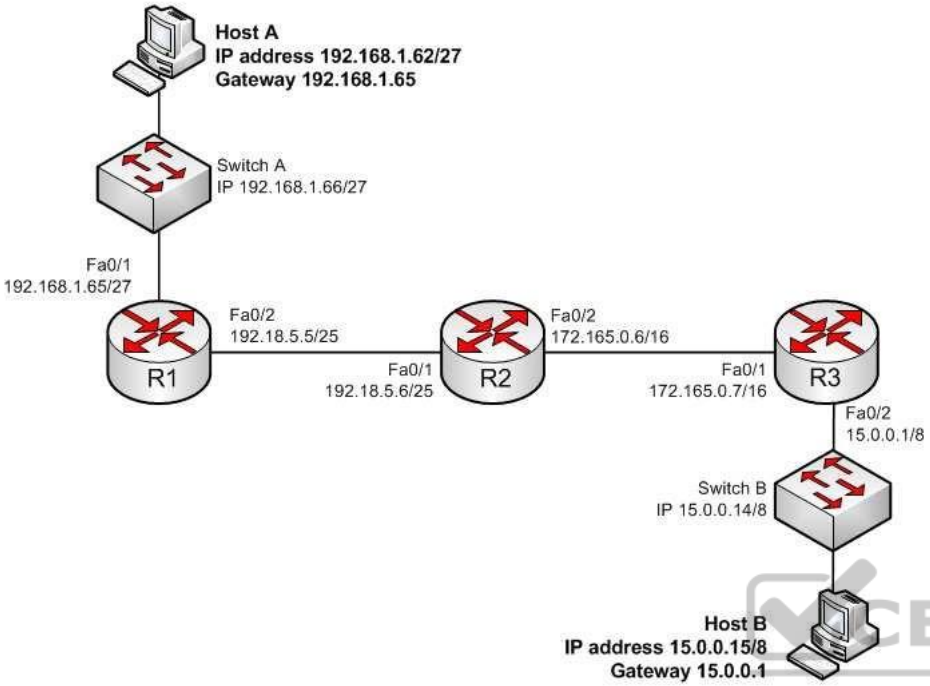
Circuit switching dynamically establishes a virtual connection between a source and destination. The virtual connection cannot be used by other callers unless the circuit is released. Circuit switching is the most common technique used with the Public Switched Telephone Network (PSTN) to make phone calls. The dedicated circuit is temporarily established for the duration of the call between caller and receiver. Once the caller or receiver hangs up the phone, the circuit is released and is made available to other users.

Packet switching is also used for data transfer but not in an ATM network. With packet switching, the data is broken into labeled packets and is transmitted using packet-switching networks. The Internet and LAN communications use packet switching.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco > Internetworking Technology Handbook > Asynchronous Transfer Mode (ATM) Switching

QUESTION 59
Examine the diagram below and assume that routing is configured properly.



Why is Host A unable to ping Host B?

A. The IP address of Switch A is incorrect
B. The gateway address of Host B is incorrect
C. The IP address of Host A is incorrect
D. The Fa0/2 and Fa0/1 interfaces on R1 and R2 are not in the same subnet

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IP address of Host A is incorrect. The Fa0/1 interface on R1 (Host A's default gateway) is in the 192.168.1.64/27 network, and Host A's IP address is in the 192.168.1.32/27 network. With a 27-bit mask against the 192.168.1.0 classful network, the resulting subnets are:

192.168.1.0

192.168.1.32
192.168.1.64
192.168.1.92

And so it would continue, increasing the fourth octet in intervals of 32. By only going this far we can see that they are in different subnets.

The IP address of Switch A is correct for its subnet because it needs to be in the same subnet as the Fa0/1 interface on R1. Even if it were incorrect or missing altogether it would have no impact on Host A. Switches merely switch frames based on MAC addresses and only need an IP address for management purposes.

The gateway address of Host B is correct. It is in the same subnet (15.0.0.0/8) with the Fa0/2 interface on R2, its gateway.

The Fa0/2 and Fa0/1 interfaces on R1 and R2 are in the same subnet. Using a 25-bit mask against the 192.18.5.0/24 classful network yields the following subnets:

192.18.5.0
192.168.5.128

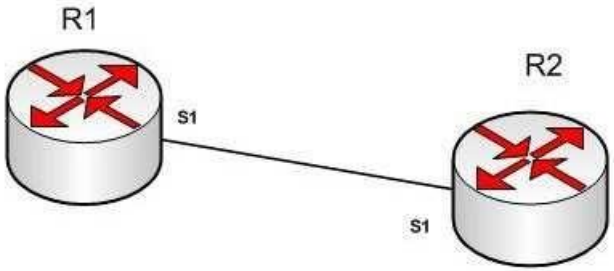
Both router interfaces in question are in the 192.18.5.0 subnet.

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

References:

Cisco > Support > IP Routing > Design TechNotes > Document ID: 13788 > IP Addressing and Subnetting for New Users

QUESTION 60
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 S1
R1(config-if)#no ip address 192.168.5.5
R1(config-if)# ip address 192.168.5.9 255.255.255.252
B. R1(config)#no ip host R1
R1(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 S1

R1(config-if)#no ip address 192.168.5.5
R1(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:

QUESTION 61
Which three statements are TRUE regarding Network Address Translation (NAT)? (Choose three.)

A. It connects different Internet Service Providers (ISPs).
B. It can act as an address translator between the Internet and a local network.
C. It conserves IP addresses.
D. It creates additional IP addresses for the local network.

E. It helps the local network connect to the Internet using unregistered IP addresses.

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NAT can act as an address translator between the Internet and the local network, conserve Internet Protocol (IP) addresses, and help the local network connect to the Internet using unregistered IP addresses.

The following statements are also TRUE regarding NAT:
- It can be used to present a single address for the entire network to the outside world when used in dynamic mode.
- It enhances network security by not disclosing the internal network addresses to the outside world.

It is not true that NAT connects different Internet Service Providers (ISPs). A gateway is used to connect different ISPs.

It is not true that NAT creates additional IP addresses for the local network. It only enables the use of unregistered addresses on the local area network.

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

References:

QUESTION 62
What is the default sequence in which a router searches for the Internetwork Operating System (IOS) image upon power on?

A. TFTP, Flash, ROM
B. ROM, Flash, TFTP
C. Flash, TFTP, ROM
D. Flash, TFTP, NVRAME. NVRAM, Flash, TFTP

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:

The default sequence in which a router searches for the IOS image is in Flash memory, on a Trivial File Transfer Protocol (TFTP) server, and in read-only memory (ROM). The router will first search for the IOS image in the Flash memory. If there is no image in the Flash, the router will try to contact a TFTP server. If the router cannot find the IOS image on the TFTP server, it will load a limited version from the ROM.

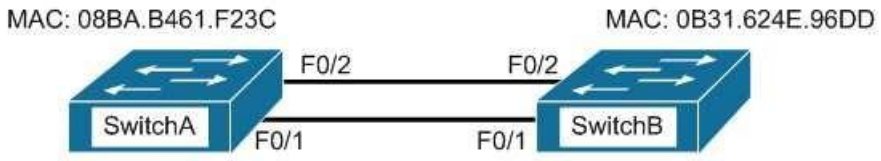
The sequence that begins with TFTP and the sequence that begins with ROM are both incorrect sequences because the router will begin searching for the IOS image in Flash memory.

The sequences that include Non-volatile random access memory (NVRAM) are both incorrect because a router does not store the IOS image in NVRAM. The startup configuration is stored in NVRAM.

Objective:
Infrastructure Management Sub-
Objective:
Perform device maintenance

References:
Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 9: Loading and Maintaining System Images > Specifying the Startup System Image in the Configuration File

QUESTION 63
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 switching loop

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

References:
Cisco > Support > LAN Switching > Spanning Tree Protocol > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w) > Document ID: 24062

QUESTION 64
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

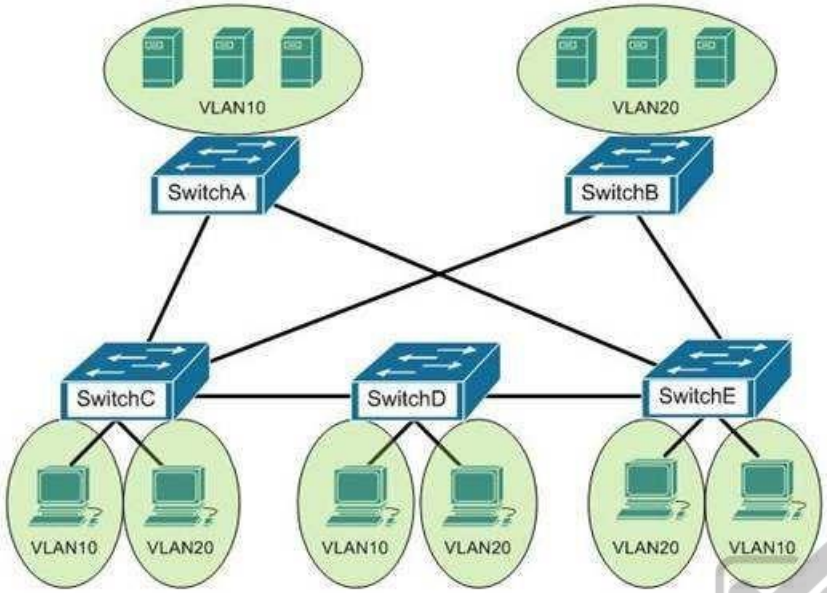
An outside local address is the IP address of an outside host as it appears to the internal network. It is not used to represent one or more inside local IP addresses externally

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:
Cisco > Support > Technology Support > IP > IP Addressing Services > Design > Design TechNotes > NAT: Local and Global Definitions
Cisco > Articles > Network Technology > General Networking > Network Address Translation

QUESTION 65
You are the switch administrator for InterConn. The network is physically wired as shown in the diagram. You are planning the configuration of STP. The majority of network traffic runs between the hosts and servers within each VLAN.



You would like to designate the root bridges for VLANS 10 and 20. Which switches should you designate as the root bridges?

A. Switch A for VLAN 10 and Switch E for VLAN 20
B. Switch A for VLAN 10 and Switch B for VLAN 20
C. Switch A for VLAN 10 and Switch C for VLAN 20
D. Switch D for VLAN 10 and Switch B for VLAN 20
E. Switch E for VLAN 10 and Switch A for VLAN 20
F. Switch B for VLAN 10 and Switch E for VLAN 20

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should designate Switch A for VLAN 10 and Switch B for VLAN 20. The STP root bridge for a particular VLAN should be placed as close as possible to the center of the VLAN. If the majority of network traffic is between the hosts and servers within each VLAN, and the servers are grouped into a server farm, then the

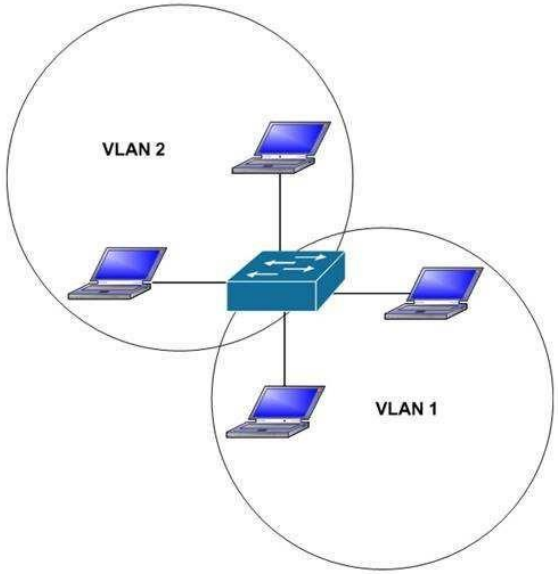
switch that all hosts will be sending their data to is the ideal choice for the STP root. Cisco's default implementation of STP is called Per-VLAN Spanning Tree (or PVST), which allows individual tuning of the spanning tree within each VLAN. Switch A can be configured as the root bridge for VLAN 10, and Switch B can be configured as the root bridge for VLAN 20, resulting in optimized traffic flow for both.

None of the other switches is in the traffic flow of all data headed towards the VLAN 20 or VLAN 10 server farms, so they would not be good choices for the root bridge for either VLAN. Care should be taken when adding any switch to the network. The addition of an older, slower switch could cause inefficient data paths if the old switch should become the root bridge.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and TechNotes > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

QUESTION 66
Which of the following statements are true with regard to the network shown in the exhibit? (Click the Exhibit(s) button.)



A. there is one broadcast domain and one collision domain

B. there is one broadcast domain and four collision domains
C. there are two broadcast domains and two collision domains
D. there are two broadcast domains and four collision domains
E. the hosts in VLAN1 could use IP addresses 192.168.5.4/24 and 192.168.5.5/24 and the hosts in VLAN2 could use IP addresses 192.168.6.1/24 and 192.168.6.2/24
F. the hosts in VLAN2 could use IP addresses 192.168.5.5/24 and 192.168.6.5/24

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are two broadcast domains and four collision domains in the network shown in exhibit. A Virtual LAN (VLAN) is a group of networking devices in the same broadcast domain. A broadcast domain is a group of devices such that when one device in the group sends a broadcast, all the other devices in the group will receive that broadcast. Because there are two VLANs shown in the exhibit, VLAN1 and VLAN2, there are two broadcast domains. A switch will not forward broadcast frames between VLANs.

A collision domain is a domain where two or more devices in the domain could cause a collision by sending frames at the same time. Each switch port is a separate collision domain. Because there are four switch ports in the exhibit, there are four collision domains.

The hosts in VLAN1 could use IP addresses 192.168.5.4/24 and 192.168.5.5/24 and the hosts in VLAN2 could use IP addresses 192.168.6.1/24 and 192.168.6.2/24. Hosts in different VLANs must have IP addresses that are in different subnets.

The other options that offer IP address plans are incorrect because they either place hosts from different VLANs in the same subnet, or place hosts in the same VLAN in different subnets.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco > Support>Technology Support > LAN Switching > Layer-Three-Switching and Forwarding > Configure > Configuration Examples and TechNotes > How To Configure InterVLAN Routing on Layer 3 Switches

QUESTION 67

Which command was used to create the following configuration?

```
Router# show ip protocol
Routing Protocol is "eigrp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: eigrp 1
Automatic network summarization is in effect
Routing for Networks:
192.168.1.80/28
192.168.1.128/28
Routing Information Sources:
Gateway Distance Last Update
192.168.1.85 90 0:04:01
Distance: internal 90 external 170
```

A. Router(config-router)# network 192.168.1.0 0.0.0.15
B. Router(config-router)# network 192.168.1.0 255.255.255.0
C. Router(config-router)# network 192.168.1.80
Router(config-router)# network 192.168.1.128
D. Router(config-router)# network 192.168.1.0

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The network 192.168.1.0 command instructs the router to activate EIGRP on every interface that belongs to the class C network 192.168.1.0. The exhibit indicates that the router is running EIGRP on two subnets of 192.168.1.0 (192.168.1.80/28 and 192.168.1.128/28). Since both of these are subnets of the same class C network number, only the class C address needs to be referenced with a network statement.

All interfaces that will participate in EIGRP must be specified with a network command that specifying the network of which the interface is a member. Failure to do so will result in neighbor relationships not forming. In the example below, Router A and Router B are directly connected, but not forming a neighbor relationship. The network they share is the 192.168.5.0/24 network. The output of the show run command for both routers reveals that Router B does not have EIGRP running on the 192.168.5.0 network.

```
RouterA#show run
<output omitted>
router eigrp 36
network 192.168.5.0
```

```
Router B#show run
<output omitted>
router eigrp 36
network 10.0.0.0
```

The network 192.168.1.0 0.0.0.15 command is incorrect because only the class C network number (192.168.1.0) needs to be referenced to enable EIGRP on all subnets. It is actually valid to include an inverse mask with EIGRP network statements, but it is unnecessary in this case, and the network/mask provided does not match either of the routed networks.

The network 192.168.1.0 255.255.255.0 command is incorrect because the mask is unnecessary in this case, and if masks are included, they must be expressed inversely (0.0.0.255).

It is unnecessary to configure two network commands in this example, as both networks are subnets of the same class C network (192.168.1.0), and a single network command can enable EIGRP on both. Additionally, if specific subnets are referenced in network commands, it is necessary to include an inverse mask after them, or EIGRP will automatically summarize the command to the classful boundary.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T > Part 3: EIGRP > Configuring EIGR

QUESTION 68
Which of the following represents the correct method of assigning an IP address and default gateway to a switch?

A. Switch(config)# interface vlan1
Switch(config-if)# ip address 10.0.0.1 255.0.0.0
Switch(config-if)# default-gateway 10.0.0.254
B. Switch(config)# ip default-gateway 10.0.0.254
Switch(config)# interface vlan1
Switch(config-if)# ip address 10.0.0.1 255.0.0.0
C. Switch(config)# ip address 10.0.0.1 255.0.0.0Switch(config)# default-gateway 10.0.0.254
D. Switch(config)# ip address 10.0.0.1 255.0.0.0Switch(config)# interface vlan1
Switch(config)# ip default-gateway 10.0.0.254

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

IP addresses are assigned to switches by assigning the address to VLAN 1 using the ip address command, while the default gateway is configured in global configuration mode using the ip default-gateway command. A default gateway is assigned to a Layer 2 switch using the following command syntax, where h.h.h.h is the IP address of the default gateway:

Switch(config)# ip default-gateway h.h.h.h

An IP address is assigned to a Layer 2 switch using the following command syntax, where h.h.h.h is the IP address and m.m.m.m is the subnet mask:

Switch(config)# interface vlan1
Switch(config-if)# ip address h.h.h.h m.m.m.m

Configuring an IP address on a switch is usually accompanied by adding a default gateway as well. Switches do not require an IP address to perform their function on the network. IP addresses are added so that an administrator can make a Telnet connection to the switch to manage the switch. If this Telnet access does not occur on the same local subnet with the switch, which is unlikely, or if the administrator is trying to Telnet to the switch using a host that resides a VLAN other VLAN1 (the management VLAN) the absence of a gateway address will render the switch incapable of answering Telnet connection attempts. Therefore, a gateway address is usually required on the switch to make a telnet connection.

The following command set is incorrect because the command setting the default gateway must be executed in global configuration mode, not in configuration mode, for VLAN1:

Switch(config)# interface vlan1
Switch(config-if)# ip address 10.0.0.1 255.0.0.0 Switch(config-if)# default-gateway 10.0.0.254

The following command set is incorrect because the IP address must be configured in configuration mode for VLAN1, not global configuration mode:

Switch(config)# ip address 10.0.0.1 255.0.0.0
Switch(config)# default-gateway 10.0.0.254

The following command set is incorrect because an IP address must be configured in configuration mode for VLAN1. Also, if you executed the command interface vlan1, the prompt would change to Switch(config-if)#. Once it did, that would be an incorrect mode for entering the default gateway.

Switch(config)# ip address 10.0.0.1 255.0.0.0
Switch(config)# interface vlan1
Switch(config)# ip default-gateway 10.0.0.254

Objective:
Infrastructure Management Sub-
Objective:
Configure and verify device management

References:

QUESTION 69
Which statement best describes a converged network?

A. a network with real-time applications
B. a network with a mix of voice, video, and data traffic
C. a network with a mix of voice and video traffic
D. a network with mix of data and video traffic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A converged network is a combination of voice, video, and data traffic. Network convergence is a migration from maintaining multiple service-specific networks, namely data voice and video, to a single IP-based network. All services are delivered on the same network, reducing infrastructure costs. Despite the benefits that network convergence provides, it is highly susceptible to network delays, especially for real-time traffic.

Converged networks frequently face the following problems:
- Bandwidth: As all the voice and video networks are combined into one universal converged network, bandwidth capacity becomes a priority.
- Packet loss: When links become congested, packets will be dropped. Voice and video traffic are intolerant of dropped packets.
- Delay: Delay represents the time it takes for packets to traverse the network and reach their destinations. While some delay is expected, delay increases when links are over-subscribed.

Voice and video traffic are intolerant of high or variable delay. A packet that arrives late is no better than a packet that does not arrive. Delays can be variable and fixed.

Fixed delays are constant and mostly induced by the computing software of the hardware devices, such as processing delay and packetization delay.

Variable delays, known as jitter, cause problems for voice and video.

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast network topologies

References:
Cisco Documentation > Internetworking Technology Handbook > Multiservice Access Technologies

QUESTION 70
The output of the show ip route command is given:

```
Router# show ip route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O 172.16.0.0 [110/5] via 10.19.24.6, 0:01:00, Ethernet2
B 172.17.12.0 [200/128] via 10.19.24.24, 0:02:22, Ethernet2
O 172.71.13.0 [110/5] via 10.19.24.6, 0:00:59, Ethernet2
O 10.13.0.0 [110/5] via 10.19.24.6, 0:00:59, Ethernet2
```

What does the value 110 in the output represent?

A. The administrative distance of the information source
B. The metric to the route
C. The type of route
D. The port number of the remote router

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The value 110 in the output represents the administrative distance (AD) of the information source. Administrative distance is used by Cisco routers to select the most trustworthy source of routing information for a particular route. Every routing protocol has a default administrative distance, and if more than one routing protocol is providing route information about a route, the protocol with the lowest AD will be selected to populate the routing table. The following table shows the AD values for different routing protocols:

IP Route	Default AD value
Connected interface	0
Static route directed to an connected interface	0
Static route directed to an IP address	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP) route	20
Internal Enhanced Interior Gateway Routing Protocol (EIGRP) route	90
Interior Gateway Routing Protocol (IGRP) route	100
Open Shortest Path First (OSPF) route	110
Intermediate System-to-Intermediate System (IS-IS) route	115
Routing Information Protocol (RIP) route	120
Exterior Gateway Protocol (EGP) route	140
On Demand Routing (ODR)	160
External Enhanced Interior Gateway Routing Protocol (EIGRP) route	170
Internal Border Gateway Protocol (BGP) route	200
Unknown origin routes	255

The following is the sample output for the show ip route command:


```
Router# show ip route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O 172.16.0.0 [110/5] via 10.19.24.6, 0:01:00, Ethernet2
B 172.17.12.0 [200/128] via 10.19.24.24, 0:02:22, Ethernet2
O 172.71.13.0 [110/5] via 10.19.24.6, 0:00:59, Ethernet2
O 10.13.0.0 [110/5] via 10.19.24.6, 0:00:59, Ethernet2
```

The following are the fields in the output:

- O: Indicates that the route was discovered using Open Shortest Path First (OSPF).
- B: Indicates that the route was discovered using Border Gateway Protocol (BGP).
- 172.16.0.0: Indicates the address of the remote network.
- 110: Indicates the administrative distance of the route.
- 128: Indicates the metric for the route.
- Via 10.19.24.6: Specifies the address of the next router in the remote network.
- 0:02:22: Indicates the last time the route was updated.
- The metric for the route is also called the cost. In the case of the OSPF routes above, the cost is 5.

The administrative distance for any particular protocol can be changed if you would like to use a routing protocol that is normally not the preferred provider. For example, if you prefer that RIP routes be installed in the routing table rather than OSPF routes, you could change the administrative distance of RIP to a lower value than OSPF (110), as shown below.

Router(config)# router rip
Router(config)# distance 100

All the other options are incorrect because they do not represent the administrative distance.

Objective:
Routing Fundamentals Sub-
Objective:
Interpret the components of routing table

References:
Cisco > Support > IP > IP Routing > Design > Design TechNotes > What Is Administrative Distance? > Document ID: 15986

QUESTION 71
In which of the following networks does the address 192.168.54.23/27 reside?

A. 192.168.54.0
B. 192.168.54.8
C. 192.168.54.4
D. 192.168.54.16

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When a class C address such as 192.168.54.0 is subnetted with a /27 mask, the subnet mask in dotted decimal format is 255.255.255.224. This means that the interval between the network IDs of the resulting subnets is 32. The resulting network IDs are as follows:

192.168.54.0
192.168.54.32
192.168.54.64
192.168.54.92 and so on.

Therefore, the address 192.168.54.23 resides in the 192.168.54.0 subnet. The address 192.168.54.0 is called a network ID or, alternately, a subnet address. It represents the subnet as a group and will be used in the routing tables to represent and locate the subnet.

Neither the first address (192.168.54.0, the network ID) nor the last address (192.168.54.31, the broadcast address) in any resulting subnet can be used. Therefore, the addresses in this range are 192.168.54.1 through 192.168.54.30, which includes the 192.168.54.23 address.

192.168.54.8 would only be a network ID if the mask were /29, which would result in an interval of 8 between network IDs. However, even if a /29 mask were used, the 192.168.54.23 address would not fall in its range. The address range for a /29 mask would be 192.168.54.9 through 192.168.54.14.

Similarly, 192.168.54.4 would only be a network ID for a /30 mask, which would result in an interval of 4 between network IDs. But even if a /30 mask were used, the 192.168.54.23 address would not fall in its range. The address range for a /30 mask would be 192.168.54.5 through 192.168.54.6.

192.168.54.16 could be a network ID if the mask were /28, /29 or /30, but not with a /27 mask.

Objective:
Network Fundamentals Sub-
Objective:
Apply troubleshooting methodologies to resolve problems

References:
Cisco > Support > IP Routing > Design TechNotes > Document ID: 13788 > IP Addressing and Subnetting for New Users

QUESTION 72
What is the primary benefit of the Virtual Local Area Network (VLAN) Trunking Protocol (VTP)?

A. broadcast control
B. frame tagging
C. inter-VLAN routing
D. consistent VLAN configuration across switches in a domain

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
VTP manages configured VLANs across a switched network and maintains consistency of VLAN information throughout a VTP domain. When an administrator adds, deletes, or renames VLANs, VTP propagates this information to all other switches in the VTP domain. This makes the process of VLAN changes a plug-andplay activity. This protocol was developed by, and remains proprietary to Cisco Systems.

Broadcast control is not the primary benefit of VTP. Broadcast control is achieved by using VLANs. VLANs segment the network into logical broadcast domains. This helps in the reduction of unnecessary traffic over the network and optimizes the available bandwidth use. VTP pruning helps reduce broadcast and unknown unicast over VLAN trunk links. However, this is not the primary benefit of VTP.

Frame tagging is required for VLAN identification as frames traverse trunk links in a switch fabric. Inter-Switch Link (ISL) and IEEE 802.1q are the two methods of frame tagging available on Cisco devices. ISL is proprietary to Cisco, whereas IEEE 802.1q is a standard method. VTP is not a frame tagging method.

Inter-VLAN routing is achieved by an Open Systems Interconnect (OSI) Layer 3 device (Router). Inter-VLAN routing is not a benefit of VTP.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco > Support > LAN Switching > Virtual LANS / VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Configuring VLAN Trunk Protocol (VTP) > Document ID: 98154
Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25) > Understanding and Configuring VLANs, VTP, and VMPS

QUESTION 73
You are the network administrator for your company and have configured Cisco Discovery Protocol (CDP) in your network. You recently noticed that when devices send large numbers of CDP neighbor announcements, some devices are crashing. You decide to disable CDP on the router.

Which command should you use to achieve the objective?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should use the no cdp run command to disable CDP on the router. Due to a known vulnerability regarding the handling of CDP by Cisco routers and switches when devices send large numbers of CDP neighbor announcements, some devices can crash or cause abnormal system behavior. To overcome this problem, you can disable CDP for the entire router by using the no cdp run command.

You cannot use the set cdp disable command to disable CDP on the router. This command disables CDP on an entire Catalyst switch.

You cannot use the no cdp enable command to disable CDP on the router. This command disables CDP on a specific interface.

You cannot use the no cdp advertise-v2 command to disable CDP on the router. This command disables CDPv2 advertisements.

Objective:

LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Support > Using Cisco Discovery Protocol
Cisco > Support > Technology Support > Network Management > Cisco's Response to the CDP Issue > Document ID: 13621

QUESTION 74
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:
Cisco > Support > Technology Support > LAN Switching > Ethernet > Design > Troubleshooting LAN Switching Environments > Document ID: 12006 > Spanning Tree Protocol

QUESTION 75
You are advising a client on the options available to connect a small office to an ISP.

Which of the following is an advantage of using an ADSL line?

A. it uses the existing cable TV connection
B. it uses the existing phone line
C. you receive a committed information rate (CIR) from the provider
D. the upload rate is as good as the download rate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: xDSL lines, including the ADSL variant, use the existing phone line and as such make installing only a matter of hooking up the DSL modem to the line.

It does not use the use the existing cable TV connection. This is a characteristic of using a cable modem rather than ADSL.

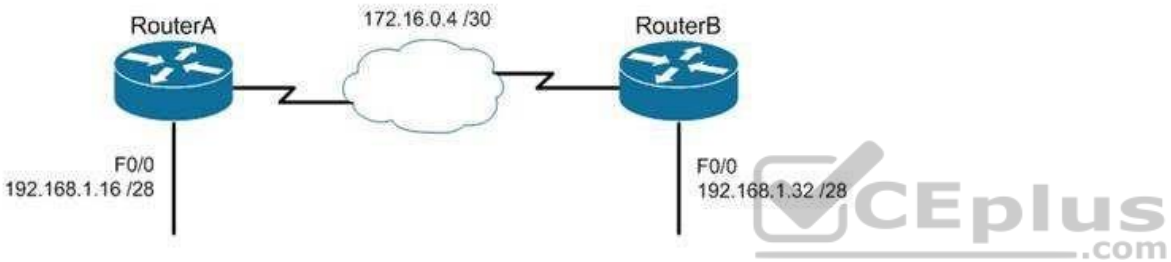
You do not receive a committed information rate (CIR) from the provider. CIR is provided with a frame relay connection.

The upload rate is NOT as good as the download rate with asynchronous DSL (ADSL). The download rate is significantly better than the upload rate. Symmetric Digital Subscriber Line (SDSL) is a version of DSL that supplies an equal upload and download rate, but that is not the case with ADSL.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies > DSL

QUESTION 76
Consider the following diagram:



Which of the following routing protocols could NOT be used with this design?

A. RIPv1
B. RIPv2
C. EIGRP
D. OSPF

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The network design displayed has subnets of a major classful network located in opposite directions from the perspective of some of the individual routers. This configuration can be accommodated by any routing protocol that supports Variable Length Subnet masks (VLSM) or the transfer of subnet mask information in routing advertisements.

RIPv1 supports neither of these. RIPv1 will automatically summarize routing advertisements to their classful network (in this case 192.168.1.0/24). This action will cause some of the routers to have routes to the same network with different next hop addresses, which will NOT work.

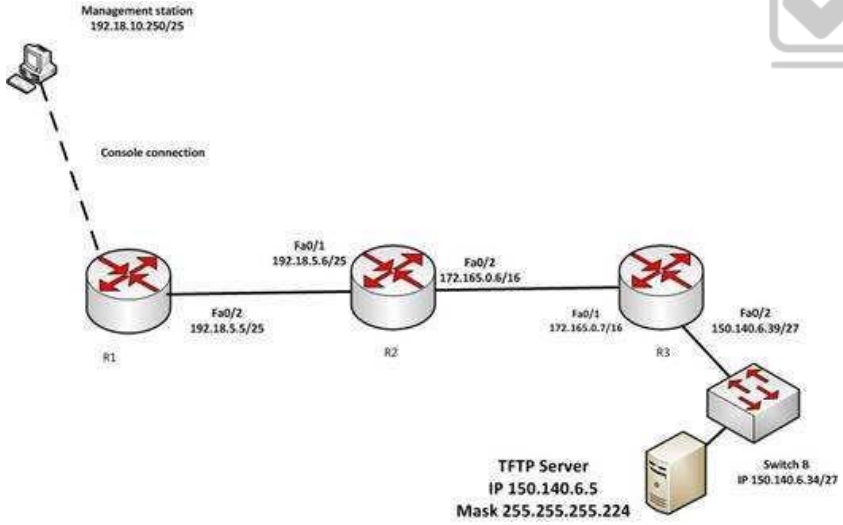
EIGRP, RIPv2 and OSPF all support VLSM and can be used in the design shown in the scenario.

Objective:
Routing Fundamentals

Sub-Objective:
Compare and contrast distance vector and link-state routing protocols

References:
Cisco > Home > Support > Technology Support > IP > IP Routed Protocols > Design > Design TechNotes > Why Don't IGRP and RIP v1 support VLSM?

QUESTION 77
You have established a console session with R1 and you are attempting to download an IOS image from the TFTP server in the diagram below.



However, you are unable to make the connection to 150.140.6.5. What is the problem?

A. The IP address of the management station is incorrect
B. The IP address of the TFTP server is incorrect
C. The interfaces between R1and R2 are not in the same subnet
D. The IP address of Switch B is incorrect

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IP address of the TFTP server is incorrect. The TFTP server, Switch B and the Fa0/2 interface on R3 should all be in the same subnet. With a 27-bit mask (255.255.255.224) against the 150.140.0.0 classful network the resulting subnets are:

150.140.0.0
150.140.0.32 150.140.0.64 and so on, incrementing in intervals of 32 in the last octet until it

reaches the 150.140.6.0 subnet.

150.140.6.0
150.140.6.32
150.140.6.64

At this point, we can see that Switch B and the router interface are in the 150.140.6.32 subnet, while the TFTP server is in the 150.140.6.0 subnet. The IP address of the TFTP server needs to be in the 150.140.6.33-150.140.6.62 range, while avoiding the addresses already used on R1 and the switch.

The IP address of the management station does not appear to be in any of the networks listed in the diagram, but that doesn't matter since the connection to the router is through the console cable which does not require a correct IP address.

The Fa0/2 and Fa0/1 interfaces on R1 and R2 are in the same subnet. Using a 25-bit mask against the 192.18.5.0/24 classful network yields the following subnets:

192.18.5.0
192.168.5.128

Both router interfaces in question are in the 192.18.5.0 subnet.

As we have already determined, the IP address of Switch B is correct. Even if it were incorrect or missing altogether, it would have no impact on connecting to the TFTP server. Switches merely switch frames based on MAC addresses and only need an IP address for management purposes.

Objective:

Routing Fundamentals Sub-
Objective:
Troubleshoot basic Layer 3 end-to-end connectivity issues

References:
Cisco > Support > IP Routing > Design TechNotes > Document ID: 13788 > IP Addressing and Subnetting for New Users

QUESTION 78
You run the following command:

```
switch# show ip interface brief
```

What information is displayed?

A. A summary of the IP addresses and subnet mask on the interface
B. A summary of the IP addresses on the interface and the interface's status
C. The IP packet statistics for the interfaces
D. The IP addresses for the interface and the routing protocol advertising the network

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The command show ip interface brief displays a summary of the IP address on the interface and the interface's status. The status shows whether the interface is up. This command is useful when you are connected to a router or switch with which you are not familiar, because it allows you to obtain the state of all interfaces or switch ports.

Sample output of this command is shown below:

```
Switch88# show ip interface brief
Interface        IP-Address OK? Method Status Protocol
FastEthernet0/1  unassigned YES manual down   down
FastEthernet0/2  unassigned YES manual down   down
FastEthernet0/3  unassigned YES manual down   down
FastEthernet0/4  unassigned YES manual down   down
FastEthernet0/5  unassigned YES manual down   down
FastEthernet0/6  unassigned YES manual down   down
FastEthernet0/7  unassigned YES manual down   down
FastEthernet0/8  unassigned YES manual up     up
FastEthernet0/9  unassigned YES manual down   down
FastEthernet0/10 unassigned YES manual down   down
```

This command does not display subnet mask information. You should use other commands, such as show ip interface or show run interface, to verify the subnet mask.

IP statistics about the interface are displayed with the command show ip interface. Adding the brief keyword tells the switch to leave out everything but the state of the interface and its IP address.

To view the routing protocol advertising an interfaces network, you would use the command show ip protocol.

Objective:
LAN Switching Fundamentals

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

References:
Cisco > Support > Cisco IOS IP Addressing Services Command Reference > show ip interface

QUESTION 79
Which command can be issued at the following prompt?

Router(config-router)#

A. show interface
B. network
C. interface
D. ip default-gateway

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The network command can be issued at the Router(config-router)# prompt, which also indicates that the router is in router configuration mode. The network command is used to configure the network upon which a routing protocol is functioning.

The router configuration mode is accessed by issuing the router command in the global configuration mode along with a parameter indicating the routing protocol to be configured. For example: R4(config)#router eigrp 1

changes the prompt to: R4(config-
router)#

which then allows you to specify the network as follows: R4(config-
router)#network 192.18.5.0

All other options are incorrect as these commands can be issued only in the global configuration command mode (which would be indicated by the R4(config)# prompt.

Objective:
Infrastructure Management Sub-
Objective:

Configure and verify initial device configuration

References:
Cisco > Support > Cisco IOS Software > Using the Command-Line Interface in Cisco IOS Software

QUESTION 80
Which of the following is NOT managed by the cloud provider in an IaaS deployment?

A. virtualization
B. servers
C. storage
D. operating system

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Operating systems are not managed by the cloud provider in an Infrastructure as a service (IaaS) deployment. Only storage, virtualization, servers, and networking are the responsibility of the provider. The customer is responsible for the following with IaaS: ▪ Operating systems
▪ Data
▪ Applications
▪ Middleware ▪
Runtime

In a Platform as a Service (PaaS) deployment, the provider is responsible for all except the following, which is the responsibility of the customer: ▪ Applications
▪ Data

In Software as a Service (SaaS) deployment, the provider is responsible for everything.

Objective:
Network Fundamentals Sub-
Objective:
Describe the effects of cloud resources on enterprise network architecture

References:
IaaS, PaaS, SaaS (Explained and Compared)

QUESTION 81
What command produced the following as a part of its output?

```
1 14.0.0.2 4 msec 4 msec 4 msec
2 63.0.0.3 20 msec 16 msec 16 msec
3 33.0.0.4 16 msec * 16 msec
```

A. Ping
B. Traceroute
C. Tracert
D. Extended ping

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The output displayed is a part of the output from executing the traceroute command. The traceroute command finds the path a packet takes while being transmitted to a remote destination. It is also used to track down routing loops or errors in a network. Each of the following numbered sections represents a router being traversed and the time the packet took to go through the router:

```
1 14.0.0.2 4 msec 4 msec 4 msec
2 63.0.0.3 20 msec 16 msec 16 msec
3 33.0.0.4 16 msec * 16 msec
```

The output would not be displayed by the ping command. This command is used to test connectivity to a remote ip address. The output from the ping command is as follows:

```
router1# ping 10.201.1.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.201.1.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```


The ping in this output was unsuccessful, as indicated by the Success rate is 0 percent output.

The output would not be displayed by the tracert command. The tracert 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, which is to test the connectivity or "reachability" of a network device or host. The tracert command uses Internet Control Message Protocol (ICMP).

The output would not be displayed by the extended version of the ping command. This command can be issued on the router to test connectivity between two remote routers. A remote execution means that you are not executing the command from either of the two routers you are interested in testing, but from a third router.

To execute an extended ping, enter the ping command from the privileged EXEC command line without specifying the target IP address. The command takes the router into configuration mode, where you can define various parameters, including the destination and target IP addresses. An example is below:

```
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

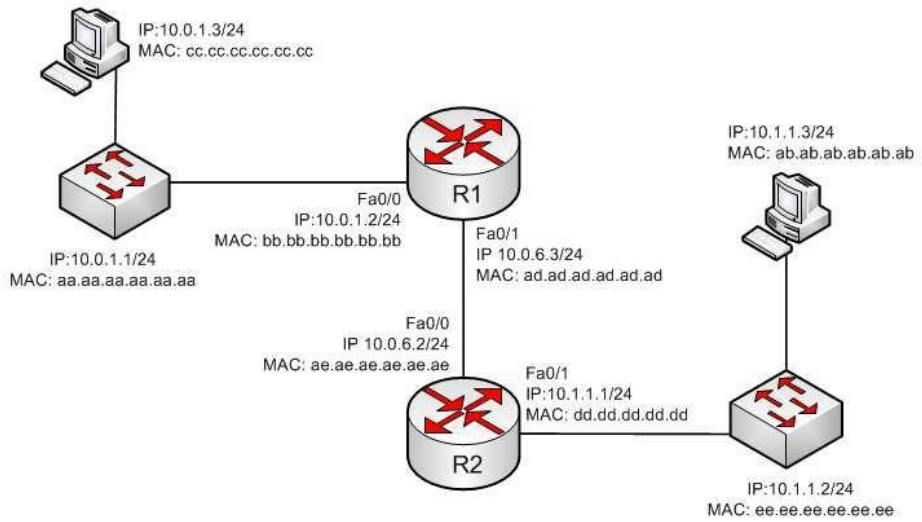
```
Extended commands [n]: y
Source address or interface: 12.1.10.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

Each line is a menu question allowing you to either accept the default setting (in parenthesis) of the ping or apply a different setting. The real value of this command is that you can test connectivity between two remote routers without being physically present at those routers, as would be required with the standard version of the ping command.

Objective:
Routing Fundamentals Sub-
Objective:
Troubleshoot basic Layer 3 end-to-end connectivity issues

References:
Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > ping
Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730 > The Extended ping Command

QUESTION 82
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 10.1.1.3
Source MAC ad.ad.ad.ad.ad.ad destination MAC ab.ab.ab.ab.ab.ab
B. source IP 10.1.1.1 destination IP 10.1.1.3
Source MAC ad.dd.dd.dd.dd.dd.dd destination MAC ab.ab.ab.ab.ab.ab
C. source IP 10.0.1.3 destination IP 10.1.1.3
Source MAC ad.ad.ad.ad.ad.ad destination MAC ae.ae.ae.ae.ae.ae
D. source IP 10.0.6.3 destination IP 10.1.1.3
Source 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:
Cisco > IOS Technology Handbook > Routing Basics

QUESTION 83
Which are among the valid steps in the process of recovering a password on a Cisco router? (Choose all that apply.)

A. Restart the router.
B. Configure the enable secret password.
C. Enter the router diagnostic mode.
D. Enter user mode.
E. Answer the security question to recover the password.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Three of the steps that should be performed while recovering a password on a Cisco router are to restart the router in ROMMOM mode, enter ROMMON mode (router diagnostic mode) and reset the enable secret password. The complete password recovery process on a Cisco Router is as follows:

Configure the router so that it starts without reading the non-volatile random access memory (NVRAM). This is also referred to as the system test mode, which you enter by changing the configuration register. You must first restart the router and within 60 seconds press Break on the terminal keyboard. Then the router will skip normal reading of the startup configuration file and will go to the ROMMON prompt (shown below this text section). At this command prompt, type confreg 0x2142

to instruct the router to boot to flash memory at the next reboot. When it does, it will ignore the startup configuration file again and will behave as if it had no configuration, as a new router would.

rommon 1> confreg 0x2142
Type reset to reboot the router.
Enter enable mode through the test system mode.
View the existing password (if it can be viewed, it may be encrypted), configure a new password, or delete the configuration.
Configure the router to start by reading the NVRAM, which is done by resetting the configuration register to its normal value. Run these commands:

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#config
Router(config)#config-register 0x2102

Restart the router.

You will proceed through user mode but to make any changes you make must be at the global configuration prompt.

Finally, there is no way to recover a password by answering a security question.

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

References:
Cisco > Home>Support>Product Support>End-of-Sale and End-of-Life Products>Cisco IOS Software Releases 12.1 Mainline>Troubleshoot and Alerts> Troubleshooting TechNotes> Password Recovery Procedures

QUESTION 84
You are the network administrator for your company. You have implemented VLAN Trunking Protocol (VTP) in your network. However, you have found that VTP is not synchronizing VLAN information.

Which of the following items should be verified to resolve the problem? (Choose three.)

A. Ensure that switches in the VTP domain are configured with VTP version 1 and version 2.
B. Ensure that VLANs are active on at least one switch on the VTP domain.
C. Ensure that all of the ports that interconnect switches are configured as trunks and are trunking properly.

D. Ensure that the VTP domain name is the same on all switches in the domain.
E. Ensure that identical passwords are configured on all VTP switches.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following is a list of the steps to take if VTP fails to exchange VLAN information:
- Ensure that all of the ports that interconnect switches are configured as trunks and are trunking properly.
- Ensure that VLANs are active in all the devices.
- Ensure that at least one switch is acting as a VTP server in the VTP domain.
- Ensure that the VTP domain name is the same for all switches in the domain. The VTP domain name is case-sensitive.
- Ensure that the VTP password is the same for all switches in the domain.
- Ensure that the same VTP version is used by every switch in the domain. VTP version 1 and version 2 are not compatible on switches in the same VTP domain.

You should not ensure that switches are configured with VTP version 1 and version 2 in the domain, because VTP version 1 and version 2 are incompatible. VTP version 1 is the default on all Cisco switches.

You should not ensure that VLANs are active on at least one switch in the VTP domain, because VLANs should be active in all of the devices in a VTP domain.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

QUESTION 85
Which of the following is NOT a possible component of Enhanced Interior Gateway Routing Protocol's (EIGRP) composite metric?

A. Cost
B. Load
C. Delay
D. Bandwidth

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Cost is not a component of EIGRP's composite metric. The cost, or efficiency, of a path is used as a metric by the Open Shortest Path First (OSPF) routing protocol.

Enhanced IGRP (EIGRP) is Cisco Systems' proprietary routing protocol. It can use bandwidth, delay, load, reliability, and maximum transmission unit (MTU) to calculate the metric. Of these five metrics, by default, only minimum bandwidth and delay are used to compute the best path.

The metric for EIGRP can be calculated with this formula:

Metric = [K1 * Bandwidth + (K2 * Bandwidth) / (256-load) + K3*Delay] * [K5 / (reliability + K4)]

The default constant values for Cisco routers are K1 = 1, K3 = 1, and K2 = 0, K4 = 0, K5 = 0. In the default setting, K1 and K3 have non-zero values, and therefore, by default, the metric is dependent on bandwidth and delay.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > IP > IP Routing > Design > Design TechNotes > Introduction to EIGRP > Document ID: 13669

QUESTION 86
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 indicates 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:

QUESTION 87
Which of the following topologies is used in Wide Area Networks (WANs)?

A. FDDI
B. CDDI
C. SONET
D. Token Ring

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Synchronous Optical NETwork (SONET) is the standard topology for fiber optic networks. Developed in 1980s, SONET can transmit data at rates of up to 2.5 gigabits per second (Gbps).

All other options are incorrect because they are LAN topologies, not WAN topologies.

Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps dual-ring fiber optics-based token-passing LAN. FDDI is typically implemented for high-speed LAN backbones because of its support for high bandwidth.

Copper Distributed Data Interface (CDDI) is copper version of FDDI. They differ only in that FDDI can span longer distances than CDDI due to the attenuation characteristics of copper wiring.

Token Ring/IEEE 802.5 LAN technology was developed by IBM in 1970. Token-ring LAN technology is based on token-passing, in which a small frame, called a token, is passed around the network. Possession of the token grants the node the right to transmit data. Once the data is transmitted, the station passes the token to the next end station.

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast network topologies

References:
Cisco>Home>Cisco Documentation > Internetworking Technology Handbook>WAN Technologies

QUESTION 88
Which of the following is the correct command to define a default route using a gateway address of 172.16.0.254?

A. ip default-route 172.16.0.254 255.255.0.0
B. ip route 0.0.0.0 0.0.0.0 172.16.0.254
C. default-gateway 172.16.0.254
D. ip route default 172.16.0.254

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The ip route command is used to manually define a static route to a destination network. The syntax of the command is as follows:

ip route [destination_network] [mask] [next-hop_address or exit interface] [administrative_distance] [permanent]

The attributes of the command are as follows:
▪ destination_network: Defines the network that needs to be added in the routing table. ▪
mask: Defines the subnet mask used on the network.
▪ next-hop_address: Defines the default gateway or next-hop router that receives and forwards the packets to the remote network. ▪
administrative_distance (AD): States the administrative distance. Static routes have an AD of 1, which can be changed to change the priority of the route.

Creating a default route is accomplished by substituting 0.0.0.0 for both the [destination_network] and [mask] fields, yielding the following command to create a default route through host 172.16.0.254:

router(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.254
Any route configured manually is considered a static route. Another example of a command that creates a non-default route is shown below:

router(config)# ip route 192.168.12.0 255.255.255.0 172.65.3.1

This command would instruct the router on which the command was executed to send any traffic for the 192.168.12.0/24 network to the router located at 172.65.3.1.

You can also affect the route by changing the administrative distance of the route. By default, all static routes have an AD of 1, making them preferable to routes learned from routing protocols. However, you can add the AD parameter at the end of the command as shown below, making the static route less desirable than one learned from a routing protocol such as RIP:

router(config)# ip route 192.168.12.0 255.255.255.0 172.65.3.1 150

One reason to configure the routes this way could be to make the static route a backup route to the route learned by RIP, such as when the static route is a less desirable route through a distant office.

Once the ip route command has been used to add either a static route or a static default route to a router, the routes should appear in the routing table. They will be indicated with an S next to a static route and an S* for a default static route. The first two examples from the explanation above would appear in the routing table as follows:

```
S*0.0.0.0/0 [1/0] via 172.16.0.254
S 192.168.12.0/24 [1/0] via 172.65.3.1
```

The ip default-route, default-gateway, and ip route default commands are incorrect because they are not valid Cisco IOS commands.

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

References:

Cisco > Cisco ASDM User Guide, 6.1 > Configuring Dynamic And Static Routing > Field Information for Static Routes
Cisco > Support > IP > IP Routing > Design > Design TechNotes > Specifying a Next Hop IP Address for Static Routes > Document ID: 27082

QUESTION 89
Which of the following statements is true with regard to SDN?

A. It combines the control plane and the data plane
B. It separates the data plane and the forwarding plan
C. It implements the control plane as software
D. It implements the data plane as software

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Software-defined networking (SDN), the control plane is separated from the data (or forwarding) plane and is implemented through software. The data plane remains on each physical device but the control plane is managed centrally for all devices though software.

SDN does not combine the data and control plane. Instead it decouples them.

SDN does not separate the data plane and the forwarding plan. These are both names for the same plane; that is, a data plane is a forwarding plane.

SDN does not implement the data plane as software. The data plane remains on each physical device.

Objective:
Infrastructure Management Sub-
Objective:
Describe network programmability in enterprise network architecture

References:
Software Defined Networking: The Cisco approach

QUESTION 90
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-configC. 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 Management Sub-
Objective:
Perform device maintenance

References:
Cisco Documentation > RPM Installation and Configuration > IOS and Configuration Basics

QUESTION 91
Which option lists the given applications in the correct sequence of increasing bandwidth consumption?

A. an interactive Telnet session on a server running an SAP application a voice conversation between PC-based VoIP services
a voice conversation between two IP phones while accessing an online video site
B. a voice conversation between two IP phones while accessing an online video site an interactive Telnet session on a server running an SAP application a voice conversation between PC-based VoIP services
C. a voice conversation between PC-based VoIP services a voice conversation between two IP phones while accessing an online video site an interactive Telnet session on a server running an SAP application

D. an interactive Telnet session on a server running an SAP application a voice conversation between two IP phones while accessing an online video site a voice conversation between PC-based VoIP services

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The correct sequence of increasing bandwidth consumption in the given scenario would be, from lowest to highest:
1. an interactive Telnet session on a server running an SAP application
2. a voice conversation between PC-based VoIP services
3. a voice conversation between two IP phones while accessing an online video site

An interactive Telnet session uses the least amount of bandwidth of the three application examples because it mainly involves the transfer of text.

A voice conversation between IP phones, also known as voice over IP (VoIP) traffic, requires more bandwidth than Telnet. Voice traffic is delay-sensitive and benefits from Quality of Service (QoS) to ensure service quality.

A voice conversation between two IP phones while accessing an online video site would consume the most bandwidth. A voice conversation with real-time video exchange is the equivalent of real-time video traffic. Video traffic is real-time and benefits from dedicated bandwidth with QoS implementation to ensure quality.

Objective: WAN
Technologies Sub-
Objective:
Describe basic QoS concepts

References:
Cisco Documentation > Internetworking Technology Handbook > Voice/Data Integration Technologies

QUESTION 92
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 nat inside 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:

QUESTION 93
How many IP addresses can be assigned to hosts in subnet 192.168.12.64/26?

A. 32
B. 62
C. 128
D. 256

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Subnet 192.168.12.64/26 has 62 IP addresses that can be assigned to hosts.

The formula to calculate the available number of hosts is:

2n - 2 = x

Where n = the number of host bits in the subnet mask and x = the number of possible hosts.

You will subtract 2 from the hosts calculation to remove the first address (the network ID) and the last address (the broadcast ID) from the valid hosts range. These addresses are reserved as the network ID and the broadcast address, respectively, in each subnet.

An IP address has 32 available bits divided into four octets. In this scenario, the /26 indicates that the subnet mask is 26 bits long, or that 26 bits are reserved for the network portion of the address. This leaves 6 bits for the host addresses (32 - 26 = 6). The number of host addresses would be calculated as follows:

Number of hosts = 26 - 2
Number of hosts = 64 - 2 = 62

Another simple way of determining the number of hosts in a range, when the subnet mask extends into the last octet, is to determine the decimal value of the last bit in the subnet mask after converting it to binary notation. This process only works when the subnet extends into the last octet, meaning that the subnet is greater than /24. The /26 subnet mask equals 26 network bits and 6 hosts bits, written as follows:

11111111.11111111.1111111.11000000

The 1s represent network bits and the 0s represent host bits.

In this example, the 26th bit (read from left to right) has a decimal value of 64, indicating that this subnet has 64 addresses. Subtract 2 to represent the network and broadcast addresses (64 - 2 = 62). This shows that this subnet range can be used to address 62 hosts.

Network address: 192.168.12.0
Subnet Mask in decimal: 255.255.255.192
Subnet Mask in binary: 11111111.11111111.11111111.11000000
Hosts: 64 - 2 = 62

For subnet 192.168.12.64, the valid host range will start from 192.168.12.65 to 192.168.12.126. For the next subnet 192.168.12.128, the valid host range will start from 192.168.12.129 to 192.168.12.190.

To construct a subnet that would contain 32 addresses would require using a mask of 255.255.255.224. This mask would leave 5 host bits, and 25 - 2 = 32.

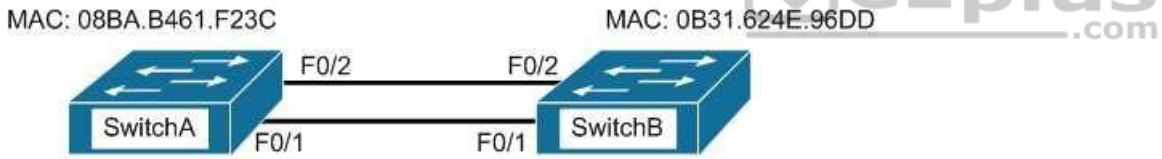
To construct a subnet that would contain 128 addresses would require using a mask of 255.255.255.128. This mask would leave 7 host bits, and 27 - 2 = 128.

To construct a subnet that would contain 256 addresses would require using a mask of 255.255.255.0. This mask would leave 8 host bits, and 2(8) - 2 = 256.

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

References:
Cisco > Design Tech Notes > IP Routing > IP Addressing and Subnetting for New Users > Understanding IP Addresses > Document ID: 13788
Nooning, Thomas. "TechRepublic Tutorial: Subnetting a TCP/IP Network." TechRepublic, 20 May 2003.

QUESTION 94
Examine the network diagram.



Which switch port(s) will be in a forwarding state? (Choose two.)

A. SwitchA - Fa0/1 and Fa0/2
B. SwitchA - Fa0/1
C. SwitchA - Fa0/2
D. SwitchB - Fa0/1
E. SwitchB - Fa0/2

Correct Answer: AD

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Both switch ports on Switch A and Fa0/1 on Switch B will be in a forwarding state. Switch A 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. Switch B has redundant connectivity to the root bridge, and must block one of its interfaces to prevent a switching loop. 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.

In this scenario there are only two switches in the diagram. However, if there were more switches and Switch A were not the root bridge, the result would be the same with regard to the ports between Swicth A and B. Whenever there are redundant links between switches, one of the four ports involved will be set to a blocking (or in the case of RSTP, discarding) mode. The logic will still be the same, since the cost to get to the root bridge will still be equal if the port speeds are equal.

Without STP (which can be disabled) operating on switches with redundant links, such as those in the figure, loops can and almost surely will occur. For example, if a host connected to SwitchA were to send an ARP request for the MAC address of a host connected to SwitchB, the request could loop and cause a broadcast storm, slowing performance dramatically. This would probably occur when any host connected to either switch sends a broadcast frame, such as a DHCP request.

Rapid Spanning Tree Protocol (RSTP) uses the term discarding for a switch port that is not forwarding frames.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and TechNotes > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

QUESTION 95
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.

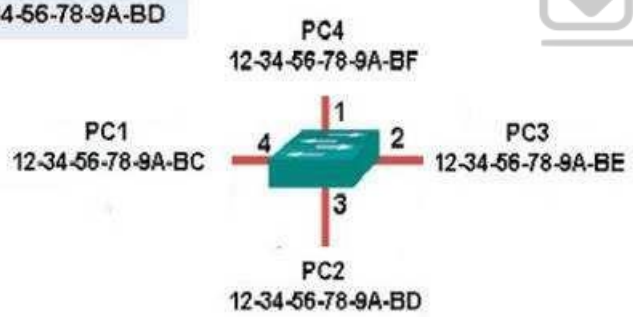
This line does not show that there is a problem at the telephone company's end. Since the interface is administratively shut down, there is no way of determining the operational status of the physical layer or protocol layer on the other end of the line.

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

References:

QUESTION 96
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:

MAC Address Table	
Port	MAC Address
1	12-34-56-78-9A-BF
3	12-34-56-78-9A-BD



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 of 12-34-56-78-9A-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 frame with 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:
Cisco Press > Articles > Cisco Certification > CCNA Routing and Switching > Basic Data Transmission in Networks: MAC Tables and ARP Tables
How do Switches Work?

QUESTION 97
Which command will display the Virtual LAN (VLAN) frame tagging method for a switch link?

A. show vlan
B. show vlan encapsulation
C. show vtp status
D. show interfaces trunk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The show interfaces trunk command displays the list of trunk ports and the configured VLAN frame tagging methods.

Sample output of the show interfaces trunk command would be as follows:

```
SwitchB# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1
Fa0/2 on 802.1q trunking 1
Fa0/3 on 802.1q trunking 1
<<output omitted>>
```

The show vlan command displays the VLAN number, name, status, and ports assigned to individual VLANs. Although the command cannot be used to determine the frame tagging method used for each trunk, it can be used to determine which ports are trunk ports by the process of elimination.

In the output below, generated from a six-port switch, the missing port (Fa0/6) is a trunk port. For communication to be possible between the two VLANs configured on the switch, Fa0/6 must be connected to a router, and trunking must be configured on the router end as well. The command is also useful for verifying that a port has been assigned to the correct VLAN as it indicates in the VLAN column the VLAN to which each port belongs.

```
Switch# show vlan

Vlan name          Status          Ports
1 default          active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
58 vlan 58         active                   Fa0/5
```


The show vlan encapsulation command is not a valid command for Cisco switches.

The show vtp status command does not display VLAN frame tagging method. The command is used to verify the status of VTP. The output of the show vtp status command would be as follows:

```
SwitchB# show vtp status
VTP Version : 2
Configuration Revision : 1
Maximum VLANs supported locally : 64
Number of existing VLANs : 16
VTP Operating Mode : Client
VTP Domain Name : MARKETING
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x4D 0x60 0xA3 0x5E 0xC7 0x41 0x8C 0x47
```

Line 6 of the given output indicates that the switch is operating in VTP Client mode. There are three possible VTP modes in which a switch can operate: Server, Client, and Transparent.

- In Server mode, any changes made in the switch, such as adding a VLAN, will be recorded in the local database and also passed on to the other switches, where the change will be added.
- In Client mode, the switch will accept and record changes from switches in Server mode, but will not accept changes made on the local switch. ▪
In Transparent mode, the switch adds changes made locally to the database, but will not send or accept changes sent from other switches.

The mode in use could be a useful piece of information during troubleshooting. For example, if you were unsuccessfully attempting to add a VLAN to the database, the reason would be that the switch is in VTP Client mode. If you were adding a VLAN in Transparent mode, the VLAN would be added to the local database but fail to appear on the other switches. If the switch were in Transparent mode, Line 6 in the above output would appear as follows:

```
VTP Operating Mode: Transparent
```

Only switches operating in VTP Server mode can accept changes to the VLAN database. This situation could be corrected easily and a VLAN 50 could be successfully added at two different configuration prompts by executing the following commands:

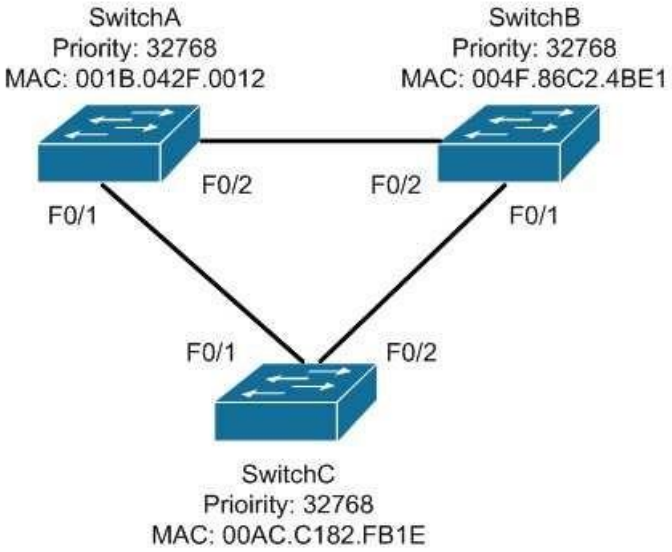
At global configuration mode:
switchB# config t
switchB(config)# vtp mode server
switchB(config)# vlan 50

At VLAN configuration mode: **switchB# vlan database switchB(vlan)#**
vtp server switchB(vlan)#
vlan 50

Objective:
LAN Switching Fundamentals Sub-Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco Press Home > Articles > Cisco Certification > CCNA > CCNA Self-Study (ICND Exam): Extending Switched Networks with Virtual LANs

QUESTION 98
View the following network diagram:



Which switch will become the root bridge?

A. SwitchA
B. SwitchB
C. SwitchC
D. The root bridge cannot be determined from the given information.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SwitchA will become the root bridge. The bridge ID, also known as the switch ID, is used to elect the root bridge in a redundant network topology. The bridge ID has two components:

- Switch's priority number: Configured as 32768 on Cisco switches by default
- Switch's Media Access Control (MAC) address: The burnt-in hardware address of the network interface card

The switch with the lowest bridge ID is selected as the root bridge. If the same priority number is configured on two or more switches in the network, the switch with the lowest MAC address will become the root. Bridge Protocol Data Units (BPDUs) communicate the details of the switch with the lowest bridge ID in the network. The election process for the root bridge takes place every time there is a topology change in the network. A topology change may occur due to the failure of a root bridge or the addition of a new switch in the network. The root bridge originates BPDUs every two seconds, which are propagated by other switches throughout the network. BPDUs are used as keepalives between switches, and if a switch stops receiving BPDUs from a neighboring switch for ten intervals (20 seconds), it will assume a designated role for the network segment.

Neither SwitchB nor SwitchC will become the root bridge. Although both have an equal priority value to SwitchA (32768), the MAC addresses of SwitchB and SwitchC are higher than that of SwitchA.

The root bridge can be determined with the information given. If the diagram did not indicate MAC addresses, then the root bridge would not be able to be determined, since the priorities are equal.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Cisco Documentation > Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX > Configuring STP and IEEE 802.1s MST > Understanding the Bridge ID
Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and TechNotes > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

QUESTION 99
Which of the following statements are true of Class C IP addresses?

A. The decimal values of the first octet can range from 192 to 223
B. The decimal values of the first octet can range from 1 to 126
C. The first octet represents the entire network portion of the address
D. The first three octets represent the entire network portion of the address
E. The value of the first binary place in the first octet must be 0
F. The value of the first two binary places in the first octet must be 11

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

Explanation:
A class C IP addresses will have the following characteristics:

- The decimal values of the first octet can range from 192 to 223
- The first three octets represent the entire network portion of the address

- The value of the first two binary place in the first octet must be 11

Class B IP addresses will have the following characteristics:
- The decimal values of the first octet can range from 128 to 191
- The first two octets represent the entire network portion of the address -
The value of the first two binary place in the first octet must be 10

Class A IP addresses will have the following characteristics:
- The decimal values of the first octet can range from 1 to 126
- The first octet represents the entire network portion of the address -
The value of the first binary place in the first octet must be 0

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast IPv4 address types

References:
Cisco > IP Routing > IP Addressing and Subnetting for New Users

QUESTION 100
Which command will save a dynamically learned MAC address in the running-configuration of a Cisco switch?

A. switchport port-security mac-address
B. switchport port-security
C. switchport port-security sticky mac-address
D. switchport port-security mac-address sticky
E. switchport mac-address sticky

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Issuing the switchport port-security mac-address sticky command will allow a switch to save a dynamically learned MAC address in the running-configuration of the switch, which prevents the administrator from having to document or configure specific MAC addresses. Once the approved MAC addresses have all been learned, the network administrator simply saves the running-configuration file to NVRAM with the copy running-config startup-config command.

Switches dynamically build MAC address tables in RAM, which allow the switch to forward incoming frames to the correct target port. 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) if additional hosts try to gain a connection. The following command secures a switch by manually defining an allowed MAC address:

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

This command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port. Manually configuring all of your switch ports in this way, however, would require documenting all of your existing MAC addresses and configuring them specifically per switch port, which could be an extremely timeconsuming task.

An example of the use of the switchport port-security mac-address sticky command is shown below:

Switch(config)#interface fastethernet0/16
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky Switch(config-if)#switchport port-security maximum 1

With the above configuration, if a computer with a MAC address of 0000.00bb.bbbb were plugged into the switch, the following two things would occur:
- Only the host with MAC address 000.00bb.bbbb will be allowed to transmit on the port. This is a result of the port-security mac-address-sticky command, which instructs the switch to learn the next MAC address it sees on the port, and of the port-security maximum 1 command, which further instructs the switch that the address learned is the only address allowed on the port.
- All frames arriving at the switch with a destination address of 0000.00bb.bbb will be forwarded out on Fa0/16.

The switchport port-security mac-address sticky command can also be used in combination with the interface-range command to make every port on the switch behave in this fashion as shown below for a 24-port switch.

Switch(config)#interface range fastethernet0/1-24
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 1

The switchport port-security mac-address command is incorrect since this command requires an additional argument to be valid (either a statically configured MAC address or the sticky option).

The switchport port-security command activates port security on the switch port, but does not configure sticky MAC address learning.

The switchport port-security sticky mac-address and switchport mac-address sticky options are incorrect because these are not valid Cisco IOS commands.

Objective:
Infrastructure Security Sub-
Objective:

Configure, verify, and troubleshoot port security

References:
Cisco > Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide > Configuring Port Security > Enabling Port Security with Sticky MAC Addresses on a Port
Cisco > Cisco IOS Security Command Reference > show vtemplate through switchport port-security violation > switchport port-security mac-address

QUESTION 101
Which of the following items are NOT required to match for two routers to form an OSPF adjacency?

A. Area IDs
B. Hello/Dead timers
C. Passwords (if OSPF authentication has been configured)
D. Process IDs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All of the listed items must match except for the process IDs. The process IDs are locally significant, which keeps multiple instances of OSPF separate on a router, and do not need to match between neighboring routers for the adjacency to form. Process identifiers can be valued from 1 to 65535.

Adjacencies must be formed before routing updates can be exchanged. OSPF routers will form neighbor adjacencies on common subnets if the following three items match:
- Area IDs
- Hello/Dead timers
- Passwords (if OSPF authentication has been configured)

Once an adjacency has been formed it will be maintained by the exchange of Hello messages. On a broadcast medium like Ethernet, they will be sent every 10 seconds. On point-to-point links, they will be sent every 30 seconds.

The show ip ospf interface interface number command can be used to display the state of the DR/BDR election process.

Consider the following output:

```
RouterA# show ip ospf interface fastethernet0/0

Fastethernet0/0 is up, line protocol is up
Internet Address 192.168.30.2/24, Area 0
Process ID 1, Router ID 192.168.45.1, Network Type BROADCAST,
Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.45.1, Interface address
192.168.30.2
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 00:00:06

RouterB# show ip ospf interface fastethernet0/0
Fastethernet0/0 is up, line protocol is up
Internet Address 192.168.30.1/24, Area 0
Process ID 2, Router ID 192.168.60.1, Network Type BROADCAST,
Cost: 10
Transmit Delay is 1 sec, State DR, Priority 2
Designated Router (ID) 192.168.60.1, Interface address
192.168.30.1
No backup designated router on this network
Timer intervals configured, Hello 30, Dead 60, Wait 40,
Retransmit 5
Hello due in 00:00:12
```


The timer intervals' configured output reveals that RouterA is showing a Hello timer of 10 seconds and a Dead timer of 40 seconds. RouterB has a Hello timer of 30 seconds and a Dead timer of 60 seconds. Hello/Dead timers have to match before OSPF routers will form an adjacency. If you executed the debug ip ospf events command on one of the routers, the router at serial /01 will not form a neighbor relationship because of mismatched hello parameters:

```
RouterA# debug ip ospf events
OSPF events debugging is on
RouterA#
*Nov 9 05:41:21.456:OSPF:Rcv hello from 10.16.2.3 area 0 from Serial0/1
```

```
192.168.35.1
*Nov 9 05:41:21.698:OSPF:Mismatched hello parameters from
192.168.35.1
```

Hellos are used to establish neighbor adjacencies with other routers. On a point-to-point network, hello packets are sent to the multicast address 224.0.0.5, which is also known as the ALLSPFRouters address.

Area IDs have to match for OSPF routers to form an adjacency. Both of these routers have the interface correctly configured in matching Area 0.

The interface priorities do not have to match for OSPF routers to form an adjacency. Interface priorities can be configured to control which OSPF router becomes the designated router (DR) or backup designated router (BDR) on a multi-access network segment.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:
Cisco > Home > Support > Technology Support > IP > IP Routing > Design > Design TechNotes > OSPF Neighbor Problems Explained

QUESTION 102
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 Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco Documentation > Cisco IOS Security Command Reference, Release 12.4 > service password-encryption
Cisco > Tech Notes > Cisco Guide to Harden Cisco IOS Devices > Document ID: 13608

QUESTION 103
You have been assigned a network ID of 172.16.0.0/26. If you utilize the first network resulting from this ID, what would be the last legitimate host address in this subnet?

A. 172.16.0.64
B. 172.16.0.63
C. 172.16.0.62
D. 172.16.0.65

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When a class B address such as 172.16.0.0 is subnetted with a /26 mask, the subnet mask in dotted decimal format is 255.255.255.192. This means that the interval between the network IDs of the resulting subnets is 64. The resulting network IDs are as follows:

172.16.0.0
172.16.0.64
172.16.0.128
172.16.0.192

172.16.1.0

and so on.

For the network ID 172.16.0.0, the last address in the range is 172.16.0.63, which is the broadcast address. Neither the network ID nor the broadcast address for any subnet can be assigned to computers. This means that the addresses that can actually be assigned range from 172.16.0.1 to 172.16.0.62. The last legitimate host address, therefore, is 172.16.0.62.

172.16.0.63 cannot be used because it is the broadcast address for the 172.16.0.0 network.

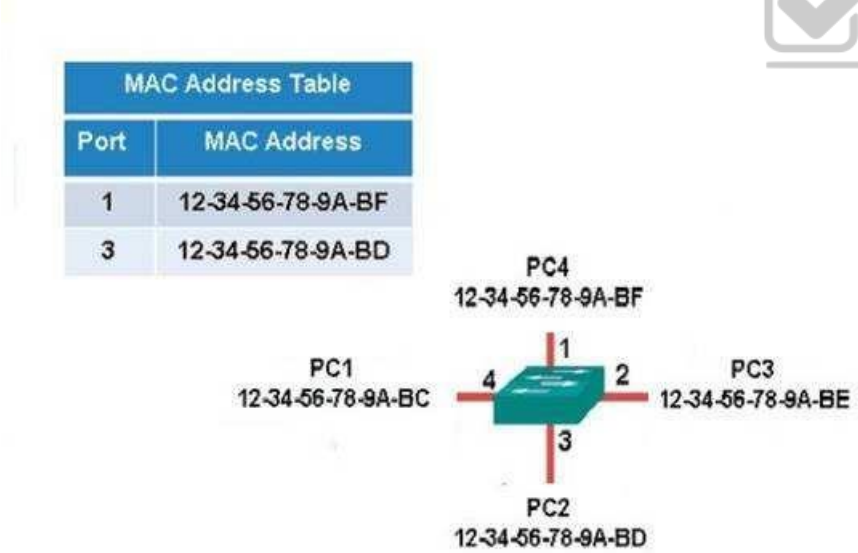
172.16.0.64 is the network ID for the 172.16.0.64 network, and 172.16.0.65 is the first address in the second network.

Objective:
Network Fundamentals Sub-
Objective:

Apply troubleshooting methodologies to resolve problems

References:
Cisco > Support > IP Routing > Design TechNotes > Document ID: 13788 > IP Addressing and Subnetting for New Users

QUESTION 104
The 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 cause the switch to add a new MAC address to its table and forward the frame to all ports when the frame is received?

A. source MAC: 12-34-56-78-9A-BC, destination MAC: ff-ff-ff-ff-ff-ff
B. source MAC: ff-ff-ff-ff-ff, destination MAC: 12-34-56-78-9A-BC
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: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:
The only frame that will be handled in the specified way is the one with a source MAC of 12-34-56-78-9A-BC and a destination MAC of ff-ff-ff-ff-ff-ff. Since the source address 12-34-56-78-9A-BC is not already in the MAC table, the switch will add it. It will forward the frame to all ports because the destination is the broadcast MAC address of ff-ff-ff-ff-ff-ff.

A frame with a source MAC of ff-ff-ff-ff-ff-ff and a destination MAC of 12-34-56-78-9A-BC is an impossible combination. That would mean that the frame is coming from all devices, which is not possible.

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

The frame with a source MAC of 12-34-56-78-9A-BC and a destination MAC of 12-34-56-78-9A-BF would not be forwarded to all ports because the destination MAC address is in the table. The switch would add a new MAC address to the table because the source MAC address is not currently in the MAC address table.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Interpret Ethernet frame format

References:
Cisco Press > Articles > Cisco Certification > CCNA Routing and Switching > Basic Data Transmission in Networks: MAC Tables and ARP Tables
How do Switches Work?

QUESTION 105
Which command is used to view the entire routing table?

A. show route-map
B. show ip mroute
C. show ip route

D. show ip protocols

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show ip route command is used to view the entire routing table. The output of this command consists of codes, gateway of last resort, directly connected networks, and routes learned through different protocols working on the network. The syntax of the show ip route command is as follows:

show ip route [address [mask] [longer-prefixes]] | [protocol [process-id]]

The parameters of the show ip route command are as follows:
▪ address: Specifies the address for which the routing information should be displayed.
▪ mask: Specifies the subnet mask. ▪ longer-prefixes: Specifies the combination of mask and address. ▪ protocol: Specifies the name of the routing protocols such as Routing Information Protocol (RIP), or Open Shortest Path First (OSPF). ▪ protocol-id: Specifies the protocol ID used to identify a process of a particular protocol.

The show route-map command is incorrect because this command is used to view the route-maps configured on the router.

The show ip mroute command is incorrect because this command is used to view the contents of the IP multicast routing table.

The show ip protocols command is incorrect because this command is used to view the routing protocols parameters, and the current timer values.

Objective:
Routing Fundamentals Sub-
Objective:
Interpret the components of routing table

References:

QUESTION 106
The conference room has a switch port available for use by the presenter during classes. Each presenter uses the same PC attached to the port. You would like to prevent any other PCs from using that port. You have completely removed the former configuration in order to start anew.

Which of the following steps are required to prevent any other PCs from using that port?

A. make the port a trunk port
B. enable port security

C. make the port an access port
D. assign the MAC address of the PC to the port
E. make the port a sticky port
F. set the maximum number of MAC addresses on the port to 1

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should create the port as an access port, enable port security, and statically assign the MAC address of the PC to the port. Creating the port as an access port ensures that the PC can use the port and port security can be enabled on the port. The second step is to enable port security, which is required to use the third command. The third command sets the MAC address of the PC as the statically assigned address on that port, meaning that only that address can send and receive on the port.

You should not make the port a trunk port. There is no need to make this a trunk port because it will not be carrying multiple VLAN traffic, only the traffic of the PC.

You should not make the port a sticky port. The sticky keyword, when used with switchport port-security 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. It will not limit the MAC addresses allowed on the port to that of the PC.

You should not set the maximum number of MAC addresses on the port to 1. That would prevent the attachment of a hub or switch to the port, but would not restrict the MAC addresses allowed on the port to the MAC address of the PC.

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

References:
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA > Configuring Port Security

QUESTION 107
You are configuring Open Shortest Path First (OSPF) protocol for IPv6 on Router5. The router has two interfaces, which have been configured as follows:

```
S0/0 - 192.168.5.1/24
S0/1 - 10.0.0.6/8
```

You would like OSPF to route for IPv6 only on the S0/0 network. It should not route for IPv6 on the S0/1 network. The process ID you have chosen to use is 25. You do not want to apply an IPv6 address yet.

Which of the following command sets would enable OSPF for IPv6 as required?

A. Router5(config)#ipv6 ospf 25
Router5(config)# network 192.168.5.0
B. Router5(config)#ipv6 ospf 25
Router5(config)#router-id 192.168.5.1
C. Router5(config)#ipv6 unicast-routingRouter5(config)#ipv6 router ospf 25
Router5(config-rtr)#router-id 1.1.1.1
Router5(config)#interface S0/0

Router5(config-if)#ipv6 ospf 25 area 0
D. Router5(config)#ipv6 unicast-routingRouter5(config)#ipv6 ospf 25
Router5(config-rtr)#router-id 1.1.1.1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The correct command sequence would be as follows:

Router5(config)# ipv6 unicast-routing
Router5(config)# ipv6 router ospf 25
Router5(config-rtr)# router-id 1.1.1.1
Router5(config)# interface S0/0
Router5(config-if)# ipv6 ospf 25 area 0

The first line enables IPv6 routing with the ipv6 unicast-routing command. The second line enables OSPF routing for IPv6 with the ipv6 router ospf command. The third assigns a necessary router ID (which was chosen at random) with the router-id command. The last two lines enable OSPF for area 0 on the proper interface.

The following command set is incorrect because it does not enable OSPF routing for IPv6, assign a necessary router ID, or enable OSPF for area 0 on the proper interface:

Router5(config)# ipv6 ospf 25
Router5(config)# network 192.168.5.0

This command set also displays incorrect use of the network command. The network command would be used with OSPF v2.

The following command set fails to enable OSPF routing for IPv6, assign a necessary router ID, or enable OSPF for area 0 on the proper interface:

Router5(config)# ipv6 ospf 25
Router5(config)# router-id 192.168.5.1

It also assigns the router ID under global configuration mode, rather than under router ospf 25 configuration mode as required.

The following command set fails to enable OSPF for area 0 on the proper interface:

Router5(config)# ipv6 unicast-routing
Router5(config)# ipv6 ospf 25
Router5(config-rtr)# router-id 1.1.1.1

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:
Cisco > Implementing OSPF for IPv6 > How to Implement OSPF for IPv6
Cisco > Cisco IOS IPv6 Command Reference > ipv6 unicast-routing
Cisco > Cisco IOS IPv6 Command Reference > ipv6 ospf area

QUESTION 108
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-demand routing, 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:
Cisco > Support > Cisco IOS IP Routing: Protocol-Independent Command Reference > show ip route

QUESTION 109
Which command would you use to see which switch interface is associated with a particular MAC address?

A. show interface mac
B. show mac
C. show mac-address-table
D. show ip interface

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show mac-address-table command displays a table of every learned MAC address, and the switch port associated with the MAC address. Sample output is as follows:

```
Switch# show mac-address-table
Mac Address Table
-------------------------------------------

Vlan Mac Address Type Ports
---- ----------- ------- -----
1 0040.63d8.ba0a DYNAMIC Fa0/1
1 0004.274c.9ca0 DYNAMIC Fa0/3
1 0040.63d8.bab8 DYNAMIC Fa0/10
1 000f.1fd3.d85a DYNAMIC Fa0/7

Total Mac Addresses for this criterion: 4
```


This output indicates that four MAC addresses have been learned by this switch, and the last column indicates the switch port over which each MAC address was learned, and for which frames destined for each MAC address will be forwarded. The MAC address table is built dynamically by examining the source MAC address of received frames. If the switch receives a MAC address not listed in this table, it will send the frame out all ports except the one from which it was originated.

The show ip interface command is a router command, and displays no information on MAC address tables.

The show interface mac and show mac commands are incorrect because they are not valid Cisco IOS commands.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Describe and verify switching concepts

References:

QUESTION 110
What command would provide the output displayed in the exhibit? (Click on the Exhibit(s) button.)

Interface	Grp	Prio	P	State	Active	Standby	Virtual IP
Vl64	2	100	P	Standby	192.168.64.10	local	192.168.64.1
Vl65	1	110	P	Active	local	192.168.65.20	192.168.65.1
Vl66	2	100	P	Standby	192.168.66.10	local	192.168.66.1
Vl67	1	110	P	Active	local	192.168.67.20	192.168.67.1
Vl68	2	100	P	Standby	192.168.68.10	local	192.168.68.1
Vl69	1	110	P	Active	local	192.168.69.20	192.168.69.1
Vl70	2	100	P	Active	local	192.168.70.20	192.168.70.1

A. switch# show hsrp
B. switch# show standby
C. switch# show interface vlan
D. switch# show standby brief

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The command show standby brief displays the output in the exhibit. It is used to display a summary of the HSRP groups of which the switch is a member. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. In the exhibit, the interface VLAN 64 is a member of HSRP group 2. Its priority in the group is 100 and it is currently the standby switch. Since preemption is configured (as indicated by the P following the priority), we know that the priority of this switch must be lower than the priority of the active device. The active device has an IP address of 192.168.64.10 and the group IP address is 192.168.64.1.

The command show standby can be used to display detailed information about HSRP groups of which a switch is a member. It does not provide the quick summary display of the exhibit. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch. The command syntax is show standby [type number [group]].

Below is an example of this command's output:

```
RouterA#show standby vlan 5

VLAN 5 - group 1
Local state is Active, priority 105, may preempt
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.10 configured
Active router is local
Standby router is 192.12.23.3 expires in 9.600
Virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:01:38
<output omitted>

VLAN 5- group 2
Local state is Standby, priority 100
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.11 configured
Active router is 192.168.23.3 expires in 9.600
Standby router is local
2 state changes, last state change 00:01:38
<output omitted>
```

In the above output, Router A is load-sharing traffic for VLAN 5. It is active for group 1 and standby for group 2. The router at address 192.168.23.3 is active for group 2 and standby for group 1. This allows traffic to be sent to both routers while still allowing for redundancy. Router A was also configured with the standby 1 preempt command (results seen in line 1), which allows it to resume its role as active for group 1 if it comes back up from an outage.

The command show interface vlan is not a complete command. A VLAN number must follow the command. When provided with a VLAN number, the output would display the status of the SVI, but no HSRP information.

The command show hsrp is not a valid command due to incorrect syntax.

Objective:
Infrastructure Services Sub-
Objective:
Configure, verify, and troubleshoot basic HSRP

References:
Cisco > Cisco IOS IP Application Services Command Reference > show standby through show udp > show standby

QUESTION 111
Which Cisco IOS command disables Cisco Discovery Protocol Version 2 (CDPv2) advertisements?

A. no cdp advertise-v2

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The no cdp advertise-v2 command disables CDPv2 advertisements. It is the reverse of the cdp advertise-v2 command, which enables CDPv2 advertisements on a device.

The no cdp v2-advertise command is not a valid Cisco IOS command.

The no cdp run command disables CDP, not CDPv2 advertisements.

The no cdp enable command disables CDP on an interface.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Support > Using Cisco Discovery Protocol

QUESTION 112
Which of the following statements are TRUE regarding EIGRP operation? (Choose two.)

A. A successor is a backup route, and is installed in both the routing and topology tables.
B. A successor is a primary route, and is installed in both the routing and topology tables.
C. A successor is a primary route, and is installed only in the routing table.
D. A feasible successor is a backup route, and is installed in both the routing and topology tables.
E. A feasible successor is a primary route, and is only installed in the routing table.
F. A feasible successor is a backup route, and is only installed in the topology table.
G. If the successor route fails and no feasible successor route exists, the router will send an update with the route marked with an unreachable metric of 16.

Correct Answer: BF

Section: (none)
Explanation

Explanation/Reference:
Explanation:
In EIGRP operations, primary or active routes are known as successors. These routes are maintained in both the routing and topology tables. The routing table is the list of network paths that are currently used by the router.

EIGRP also has the ability to maintain backup routes to destination networks. These backup routes are known as feasible successors. If a feasible successor is discovered by EIGRP, it will be maintained only in the topology table, since it is not currently being used to route traffic. In the event of a successor failure, the backup feasible successor will become the successor, and will be installed in the routing table automatically. If the successor route fails and no feasible successor route exists, the router will send queries to all neighbors until a new successor is found.

EIGRP maintains three dynamic tables in RAM:
▪ Neighbor table, which is a list of all neighboring EIGRP routers on shared subnets ▪
Topology table, which contains all discovered network paths in the internetwork
▪ Routing table, which contains the best path (based on lowest metric) to each destination network

A successor is not a backup route. A successor is a primary or active route, and it is stored in both the routing and topology tables.

A feasible successor is not a primary route. It is a backup route, and it is stored only in the topology table.

If the successor route fails and no feasible successor route exists, the router will not send an update with the route marked with an unreachable metric of 16. EIGRP does not send an update with the route marked with an unreachable metric, and even if it did, 16 is not an unreachable metric in EIGRP as it is in RIP. Instead it sends a multicast query packet to all adjacent neighbors requesting available routing paths to the destination network.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > Enhanced Interior Gateway Routing Protocol > Document ID: 16406 > Feasible Distance, Reported Distance, and Feasible Successor

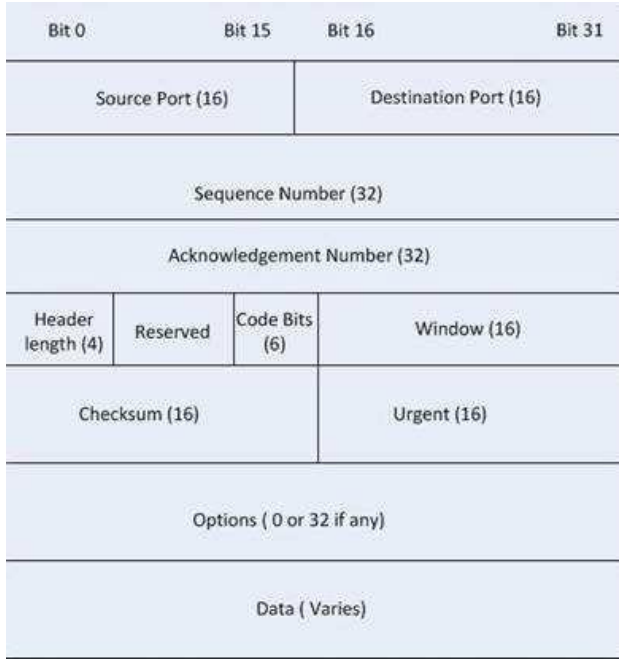
QUESTION 113
What data structure is pictured in the graphic?

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:
Cisco > Home > Internetworking Technology Handbook > Internet Protocols > User Datagram Protocol (UDP)

QUESTION 114
Which of the following excerpts from the output of the show ip eigrp topology command include EIGRP learned routes or pairs of routes that will be included in the routing table? (For excerpts that include multiple routes, do not include the entry unless BOTH routes will be included in the routing table.)

A. P 172.16.16.0/24, 1 successors, FD is 284244via
172.16.250.2 (284244/17669856), Serial0/0 via
172.16.251.2 (12738176/27819002), Serial0/1
B. P 172.16.250.0/24, 1 successors, FD is
2248564via Connected, Serial0/0
C. P 172.16.10.0/24 2 successors, FD is 284244via
172.16.50.1 (284244/17669856), Serial1/0 via
172.16.60.1 (284244/17669856), Serial1/1
D. P 172.16.60.0/24, 1 successors, FD is
2248564via Connected, Serial1/1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following excerpt indicates two successor routes, and they will both be included:

P 172.16.10.0/24 2 successors, FD is 284244
via 172.16.50.1 (284244/17669856), Serial1/0
via 172.16.60.1 (284244/17669856), Serial1/1

Both of these routes will be included because they have identical metrics (284244/17669856). Only the EIGRP successor routes will appear in the routing table, as these are considered the best-path routes to each remote network.

The route for 172.16.16.0/24 via 172.16.251.2 (12738176/27819002) will not be included because only successor routes are included, and this route is a feasible successor. Feasible successor routes are routes that are used only as a backup if the successor route(s) becomes unavailable. If you examine the output of each option, it will indicate how many successor routes are in the entry. The entry shows that there is only one successor to this route:

P 172.16.16.0/24, 1 successors, FD is 284244
via 172.16.250.2 (284244/17669856), Serial0/0
via 172.16.251.2 (12738176/27819002), Serial0/1

The first listed is the successor and the second is the feasible successor. The first has the best or lowest metric (284244/17669856), which is the criterion used for selection.

These entries indicate successor routes, but they also indicate they are via Connected, which means they are networks directly connected to the router.

P 172.16.250.0/24, 1 successors, FD is 2248564
via Connected, Serial0/0

and

P 172.16.60.0/24, 1 successors, FD is 2248564
via Connected, Serial1/1

Therefore, they are not EIGRP learned routes.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Cisco IOS IP Routing Protocols Command Reference > EIGRP Commands: M through V > show ip eigrp topology

QUESTION 115
Which of the following characteristics are NOT shared by RIPv1 and RIPv2?

A. They share an administrative distance value
B. They use the same metric
C. They both send the subnet mask in routing updates
D. They have the same maximum hop count

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
RIPv1 and RIPv2 do NOT both send the subnet mask in routing updates. RIPv1 is classful, while RIPv2 is classless. This means the RIPv1 does not send subnet mask information in routing updates, while RIPv2 does.

Both versions have the same administrative distance of 120.

Both versions have the same metric, which is hop count.

Both versions have the same maximum hop count, which is 15.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)

References:
Home > Knowledgebase > Cisco Certified Network Associate (CCNA) > Difference between RIPv1 and RIPv2
Cisco Press > Articles > Cisco Certification > CCDA > CCDA Self-Study: RIP, IGRP, and EIGRP Characteristics and Design

QUESTION 116
Which Enhanced Interior Gateway Routing Protocol (EIGRP) packet is NOT sent reliably over the network?

A. Update
B. Query
C. Reply
D. Acknowledgement

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Acknowledgement packets are sent unreliably over the network, and there is no guaranteed delivery of acknowledgement packets between neighboring routers.

Acknowledgement packets are a special type of hello packets that do not contain data and have a non-zero acknowledgement number. These are sent as a unicast.

Update, Query, and Reply packets use Reliable Transport Protocol (RTP), which ensures guaranteed delivery of packets between neighboring devices. The RTP mechanism ensures loop-free synchronized network.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Internetworking Technology Handbook > Enhanced Interior Gateway Routing Protocol (EIGRP)

QUESTION 117

You recently implemented SNMPv3 to increase the security of your network management system. A partial output of the show run command displays the following output that relates to SNMP:

```
<output omitted> snmp-server group TECHS v3 noauth read

TECHS write TECHS
```

Which of the following statements is true of this configuration?

A. It provides encryption, but it does not provide authentication
B. It provides neither authentication nor encryption
C. It provides authentication, but it does not provide encryption
D. It provides both authentication and encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
It provides neither authentication nor encryption. In SMNPv3, there are three combinations of security that can be used:
▪ noAuthNoPriv- no authentication and no encryption; includes the noauth keyword in the configuration ▪
AuthNoPriv - messages are authenticated but not encrypted; includes the auth keyword in the configuration
▪ AuthPriv - messages are authenticated and encrypted; includes the priv keyword in the configuration

In this case, the keyword noauth in the configuration indicates that no authentication and no encryption are provided. This makes the implementation no more secure than SNMPv1 or SNMPv2.

In SNMPv1 and SNMPv2, authentication is performed using a community string. When you implement SNMP using the noauth keyword, it does not use community strings for authentication. Instead it uses the configured user or group name (in this case TECHS). Regardless, it does not provide either authentication or encryption.

Objective:
Infrastructure Management Sub-
Objective:
Configure and verify device-monitoring protocols

References:
SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) > SNMPv3

QUESTION 118
You are the network administrator for your company. You want to upgrade the network, which is currently running on IPv4, to a fully functional IPv6 network. During the transition, you want to ensure that hosts capable only of IPv6 can communicate with hosts capable only of IPv4 on the network.

Which solution should you implement to accomplish the task in this scenario?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The protocol translation deployment model should be used to accomplish the task in this scenario. It is the only offered solution that does not require at least one end of the communication solution to support both IPv6 and IPv4.

The following deployment models are available for IPv4 to IPv6 migration:
- IPv6 over IPv4 tunnels: IPv6 traffic is encapsulated into IPv4 packets. Then these packets are transferred over 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 the edge router at each end be capable of both protocols.
- Protocol translation: A method 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 communication 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:

QUESTION 119
Which Cisco Internetwork Operating System (IOS) command is used to make the running configuration in Random Access Memory (RAM) to the configuration the router will use at startup?

A. copy running-config startup-config
B. copy flash running-config
C. copy tftp flash
D. copy running-config flash memory
E. copy startup-config tftp
F. copy tftp running-config
G. copy running-config tftp

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The copy running-config startup-config command is used to make the running configuration in Random Access Memory (RAM) the configuration the router will use at startup. It saves the running configuration in RAM to the router's NVRAM. This command should always follow changes to the configuration; otherwise, the changes will be lost at the next router restart. The startup configuration loads into memory from NVRAM at boot and resides in memory. When the router restarts, memory information is lost.

The copy flash running-config command is incorrect because this would copy a configuration from the router's flash memory to the running configuration, causing it to be the active configuration. While this can be done, it is not a common practice. Configuration files are normally stored in NVRAM.

The copy tftp flash command is incorrect because this command is used to replace the IOS image with a backup IOS image stored on a TFTP server to the target router. A router can also act as a TFTP server for another router. When you execute this command, you will be prompted for the IP address or hostname of the TFTP server. This prompt will display as in this example:

```
router#enable
router#copy tftp flash
Address or name of remote host []? 192.168.1.5.2
```

Before performing an upgrade of the IOS version from a TFTP server, you should verify that the upgrade is necessary by verifying the current IOS version number. The IOS version number can be found in the output of the following commands:

- **show running-config**
- **show version** - **show flash**

The copy running-config flash memory command is incorrect because this command would copy the running configuration to the router's flash memory. It is the opposite of the copy flash-running config command. While this can be done, it is not a common practice. Flash is typically used to store the Cisco IOS or operating system. Configuration files are normally stored in NVRAM.

The copy startup-config tftp command is incorrect because this command would be used to copy the current configuration stored in NVRAM to a TFTP server. When you execute this command, you will be prompted for the IP address or hostname of the TFTP server. This prompt will display as below:

router#copy start tftp
Address or name of remote host []? 192.168.1.5
Destination filename [router-confg]?

The address 192.168.1.5 is the address of the TFTP server. If no file name is given, it will save the file as router-config.

The copy tftp running-config is incorrect. This command is used to merge a backup configuration located on a TFTP server with the configuration in RAM.

The copy running-config tftp command in incorrect. It is used to make a backup copy of the configuration residing in RAM to a TFTP server.

Objective:
Infrastructure Management Sub-
Objective:
Perform device maintenance

References:
Cisco > Tech Notes > How To Copy a System Image from One Device to Another > Document ID: 15092
Cisco Documentation > Cisco IOS Release 12.4 Command References > Using Cisco IOS Software for Release 12.4 > Understanding Command Modes

QUESTION 120
Which of the following is NOT a benefit of cloud computing to cloud users?

A. On-demand self-service resources provisioning
B. Centralized appearance of resources
C. Highly available, horizontally scaled applications
D. Cost reduction from standardization and automation

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Cost reduction from standardization and automation is a benefit that accrues to the cloud provider, not the cloud users. Additional benefits to cloud providers are:
- High utilization through virtualization and shared resources
- Easier administration
- Fail-in-place operations model

Benefits that accrue to cloud users include:
- On-demand self-service resources provisioning
- Centralized appearance of resources
- Highly available, horizontally scaled applications
- No local backups required

Cloud users can also benefit from new services such as intelligent DNS, which can direct user requests to locations that are using fewer resources.

Objective:
Network Fundamentals Sub-
Objective:
Describe the effects of cloud resources on enterprise network architecture

References:
Cloud and Systems Management Benefits

QUESTION 121
When the auth keyword is used in the snmp-server host command, which of the following must be configured with an authentication mechanism?

A. the interface
B. the host
C. the user
D. the group

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The auth keyword specifies that the user should be authenticated using either the HMAC-MD5 or HMAC-SHA algorithms. These algorithms are specified during the creation of the SNMP user.

For example, the following command creates a user named V3User who will be a member of the SNMP group V3Group and will use HMAC-MD5 with a password of Password: `snmp-server user V3User V3Group v3 auth md5 Password`

The authentication mechanism is not configured on the interface. All SNMP commands are executed at the global configuration prompt.

The authentication mechanism is not configured at the host level. The version and security model (authentication, authentication and encryption, or neither) are set at the host level.

The authentication mechanism is not configured at the SNMP group level. The group level is where access permissions like read and write are set. This is why a user account must be a member of a group to derive an access level, even if it is a group of one.

Objective:
Infrastructure Management Sub-
Objective:
Configure and verify device-monitoring protocols

References:
Configuring SNMP Support > Understanding SNMP > SNMP Versions
Cisco IOS Network Management Command Reference > snmp-server engineID local through snmp trap link-status > snmp-server host

QUESTION 122
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 autoconfiguration 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:
Cisco > Understanding IPv6 Link Local Address

QUESTION 123
Multiple routes to a destination already exist from various routing protocols.

Which of the following values is used FIRST to select the route that is inserted into the route table?

A. composite metric
B. administrative distance
C. prefix length
D. hop count

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

When multiple routes to a destination exist from various routing protocols, the first value to be evaluated is the administrative distance of the source of the route. The following are examples of default administrative distance values:

Connected	0
Static	1
eBGP	20
EIGRP(internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP(external)	170
iBGP	200
EIGRP summary route	5

The second value to be compared is the composite metric, or any metric value for that matter. It is only used when multiple routes exist that have the same administrative distance.

The prefix length is only used to compare two existing routes in the routing table that lead to the destination, yet have different mask or prefix lengths. In that case, the route with the longest prefix length will be chosen.

Hop count is ONLY used when comparing multiple RIP routes. It is not the first consideration when multiple routes from various routing protocols exist in a routing table.

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

References:
Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Configuration Example and TechNotes > Route Selection in Cisco Routers

QUESTION 124
When executed on a HSRP group member named Router 10, what effect does the following command have?

```
Router10(config-if)# standby group 1 track serial0 25
```

A. It will cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down
B. It will cause the router to shut down the Serial0 interface if 25 packets have been dropped

C. It will cause the router to notify Router 25 is serial 0 goes down
D. It will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This command will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down. Interface tracking can be configured in Hot Standby Routing Protocol (HSRP) groups to switch traffic to the standby router if an interface goes down on the active router. This is accomplished by having the active router track its interface. If that interface goes down, the router will decrement its HSRP priority by the value configured in the command. When properly configured, this will cause the standby router to have a higher HSRP priority, allowing it to become the active router and to begin serving traffic.

When the standby router in an HSRP group is not taking over the active role when the active router loses its tracked interface, it is usually a misconfigured decrement value, such that the value does not lower the HSRP priority of the active router far enough for the standby to have a superior priority value.

The command will not cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down. HSRP routers track their own interfaces, not those of another router.
The command will not cause the router to shut down the Serial0 interface if 25 packets have been dropped. It will only do this if the link becomes unavailable.

The command will not cause the router to notify Router 25 is serial 0 goes down. The number 25 in the command is the decrement value, not the ID of another router.

Objective:
Infrastructure Services Sub-
Objective:
Configure, verify, and troubleshoot basic HSRP

References:
Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands
Cisco > Cisco IOS IP Application Services Command Reference > standby track

QUESTION 125
Which of the following commands will enable a global IPv6 address based on the Modified EUI-64 format interface ID?

A. ipv6 address 5000::2222:1/64
B. ipv6 address autoconfig

C. ipv6 address 2001:db8:2222:7272::72/64 link-local
D. ipv6 enable

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
To configure the interface to create a global IPv6 address based on the Modified EUI-64 format interface ID, you must enable stateless autoconfiguration. In stateless autoconfiguration, the interface will receive the network prefix from the router advertisement (RA) and generate a full IPv6 address by spreading the 48-bit MAC address of the interface across 64 bits to complete the address. This can all be done simply by executing the ipv6 address autoconfig command at the interface configuration prompt.

The command ipv6 address 5000::2222:1/64 is used to manually assign a full IPv6 address to the interface without using stateless autoconfiguration or the eui-64 keyword to manually specify the first 64 bits and allow the last 64 bits to be generated from the MAC address of the interface.

The command ipv6 address 2001:db8:2222:7272::72/64 link local is used to configure a link-local address manually without allowing the system to generate one from the MAC address, which is the default method.

The command ipv6 enable is used to allow the system to generate a link-local address from the MAC address. Because this is the default behavior, the command is not required if any other ipv6 commands have been issued. Regardless of how many manual IPv6 addresses you configure, a link local address is always generated by default.

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

References:
Cisco > Product Support > Security > Cisco ASA 5500-X Series Firewalls > Configure > Configuration Guides > Cisco Security Appliance Command Line Configuration Guide, Version 7.2 > Chapter: Configuring IPv6 > Enforcing the Use of Modified EUI-64 Interface IDs in IPv6 Addresses Cisco > Support > Cisco IOS IPv6 Command Reference > ipv6 address

QUESTION 126
Which statement is TRUE of the CSMA/CD Ethernet media access method?

A. It requires centralized monitoring and control.
B. It is ideal for a switched network environment.
C. It uses a back-off algorithm to calculate a random time value.

D. Each station is allotted a time slot in which they can transmit data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Carrier Sense Multiple Access - Collision Detection (CSMA/CD) Ethernet Media Access Control (MAC) method uses a back-off algorithm to calculate random times to transmit packets across a channel. When two stations start transmitting at same time, their signals will collide. The CSMA/CD method detects the collision and causes both stations to hold the retransmission for an amount of time determined by the back-off algorithm. This is done in an effort to ensure that the retransmitted frames do not collide.

CSMA/CD does not require centralized monitoring and control nor does it assign time slots to stations. Moreover, the CSMA/CD method is designed to work in nonswitched environment. It is an alternative to a token-passing topology, in which each station waits in turn to receive a token that allows it to transmit data. With CSMA/CD, each station is capable of making the decision regarding when to transmit the data.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Describe and verify switching concepts

References:
Cisco Documentation > Internetworking Technology Handbook > Ethernet Technologies

QUESTION 127
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:
Apply troubleshooting methodologies to resolve problems

References:
Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

QUESTION 128
Which is the shortest possible notation of the following Internet Protocol version 6 (IPv6) address?

`2001:0DB8:0000:0001:0000:0000:0000:F00D`

A. 2001:DB8::1::F00D
B. 2001:DB8:0:1::F00D

C. 2001:DB8:0:1:0:0:0:F00D
D. 2001:0DB8:0:1::F00D

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The shortest possible notation of the IPv6 address 2001:0DB8:0000:0001:0000:0000:0000:F00D is 2001:DB8:0:1::F00D. The address is shortened according to the following rules:
▪ Remove leading zeros.
▪ Remove the consecutive fields of zeros with double colon (::). ▪
The double colon (::) can be used only once.

The option 2001:DB8::1::F00D is incorrect because the double colon (::) can be used only once in the process of shortening an IPv6 address.

The option 2001:DB8:0:1:0:0:0:F00D is incorrect because 2001:DB8:0:1:0:0:0:F00D can be further shortened to 2001:DB8:0:1::F00D.

The option 2001:0DB8:0:1::F00D is incorrect because 2001:0DB8:0:1::F00D can be further shortened to 2001:DB8:0:1::F00D.

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast IPv6 address types

References:

QUESTION 129
You have connected two routers in a lab using a Data Terminal Equipment (DTE)-to-Data Circuit-terminating Equipment (DCE) cable.

Which command must be issued on the DCE end for the connection to function?

A. bandwidth
B. no clock rate
C. clock rate
D. no bandwidth

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should issue the clock rate command on the DCE end for the connection to function. The clock rate is set on the Data Circuit-terminating Equipment (DCE) device. DCE is also known as Data Communications Equipment.

The DCE terminates a physical WAN connection, provides clocking and synchronization of a connection between two locations, and connects to a DTE. The DCE category includes equipment such as CSU/DSUs, NT1s, and modems. In the real world, the clock rate is provided by the CSU/DSU end at the telcom provider. In a lab, you must instruct the DCE end to provide a clock rate.

The DTE is an end user device, such as a router or a PC, which connects to the WAN via the DCE device.

You would not issue the bandwidth command. This command is used to inform the router of the bandwidth of the connection for purposes of calculating best routes to locations where multiple routes exist. It is not necessary for the link described to function.

You should not issue the no clock rate command. This command is used to remove any previous settings implemented with the clock rate command.

You would not issue the no bandwidth command. This command is used to remove any previous settings implemented with the bandwidth command

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco IOS Software Releases 11.1 > Configure > Feature Guides > Clock Rate Command Enhancements Feature Module
CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 12: Point-to-Point WANs, pp. 446-447.

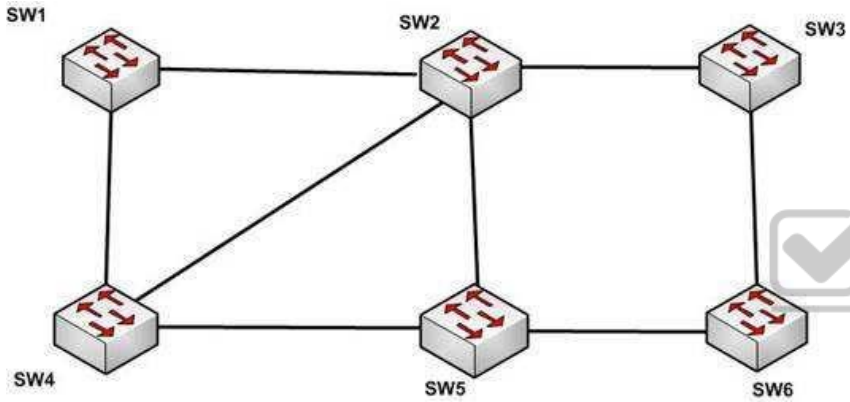
QUESTION 130
Why is it recommended to use Spanning Tree Protocol (STP) in Local Area Networks (LANs) with redundant paths?

A. To prevent loops
B. To manage VLANs
C. To load balance across different paths
D. To prevent forwarding of unnecessary broadcast traffic on trunk links

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Spanning Tree Protocol (STP) is a Layer 2 protocol used in LANs to maintain a loop-free network topology by recognizing physical redundancy in the network and logically blocking one or more redundant ports.

An example of switch redundancy is shown in the diagram below. The connection from SW4 to SW2, while providing beneficial redundancy, introduces the possibility of a switching loop.



STP probes the network at regular intervals to identify the failure or addition of a link, switch, or bridge. In the case of any topology changes, STP reconfigures switch ports to prevent loops. The end result is one active Layer 2 path through the switch network.

STP is not used for management of Virtual Local Area Networks (VLANs). VLAN Trunking Protocol (VTP) simplifies the management of VLANs by propagating configuration information throughout the switching fabric whenever changes are made. In the absence of VTP, switch VLAN information would have to be configured manually.

STP is not used to load-balance traffic across different redundant paths available in a topology. Load balancing allows a router to use multiple paths to a destination network. Routing protocols, Routing Information Protocol (RIP), RIPv2, Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) support load balancing. Similarly, multiple links can be combined in a faster single link in switches. This can be achieved with the Fast EtherChannel or Gigabit EtherChannel features of Cisco switches.

STP does not prevent forwarding of unnecessary broadcast traffic on trunk links. This is achieved by manually configuring VLANs allowed on the trunk, or through VTP pruning.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Cisco > Support > Configuring Spanning Tree-Protocol > How STP Works

QUESTION 131
Enhanced Interior Gateway Routing Protocol (EIGRP) uses which algorithm to select the best path to the destination?

A. Diffusing Update Algorithm (DUAL)

B. Dijkstra algorithm
C. Bellman-Ford algorithm
D. Shortest Path First (SPF) algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
EIGRP uses the Diffusing Update Algorithm (DUAL) to select the best path to the destination. EIGRP is a classless protocol that allows the use of variable length subnet masks (VLSM), and supports classless interdomain routing (CIDR) for the allocation of IP addresses.

EIGRP is characterized by these components:
- DUAL: EIGRP implements DUAL to select paths free of routing loops. DUAL selects the best path and the second best path to the destination. The terminology used in DUAL is as follows:
  - Successor: Best path selected by DUAL.
  - Feasible successor: Second best path selected by DUAL. This is a backup route stored in the topology table. - Feasible distance: The lowest calculated metric of a path to destination.
- Protocol-dependent modules: Different modules are used by EIGRP to independently support Internet Protocol (IP), Internetwork Packet Exchange (IPX), and AppleTalk routed protocols. These modules act as a logical interface between DUAL and routing protocols.
- Neighbor discovery and recovery: Neighbors are discovered and information about neighbors is maintained by EIGRP. A hello packet is multicast on 224.0.0.10 every five seconds and the router builds a table with the information. EIGRP also enables proper operation over a Non-Broadcast Multiple Access (NBMA) pointto-multipoint network. EIGRP multicasts a hello packet every 60 seconds on the multipoint Wide Area Network (WAN) interfaces (X.25, frame relay, or Asynchronous Transfer Mode).
- Reliable Transport Protocol (RTP): RTP is used by EIGRP to manage EIGRP packets. Reliable and ordered delivery of route updates is ensured using RTP.

EIGRP updates about routes can contain five metrics: minimum bandwidth, delay, load, reliability, and maximum transmission unit (MTU). Of these five metrics, by default, only minimum bandwidth and delay are used to compute the best path.

The Dijkstra algorithm and Shortest Path First (SPF) algorithm are used by the Open Shortest Path First (OSPF) routing protocol for selecting the best path to the destination, not by EIGRP.

The Bellman-Ford algorithm is used by Routing Information Protocol (RIP).

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast interior and exterior routing protocols

References:
Cisco > Internetworking Technology Handbook > Enhanced Interior Gateway Routing Protocol (EIGRP)

QUESTION 132
You have been asked to troubleshoot the NTP configuration of a router named R70. After executing the show run command, you receive the following partial output of the command that shows the configuration relevant to NTP:

```
clock timezone PST -8 clock
summer-time PDT recurring ntp
update-calendar ntp server
192.168.13.57 ntp server
192.168.11.58 interface
Ethernet 0/0 ntp broadcast
```


Based on this output, which of the following statements is true?

A. the time zone is set to 8 hours less than Pacific Standard time
B. the router will listen for NTP broadcasts on interface E0/0
C. the router will send NTP broadcasts on interface E0/0
D. the router will periodically update its software clock

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The router will send NTP broadcast on its E0/0 interface. The command ntp broadcast, when executed under an interface, instructs the router to send NTP broadcast packets on the interface. Any devices on the network that are set with the ntp broadcast client command on any interface will be listening for these NTP broadcasts. While the clients will not respond in any way, they will use the information in the NTP broadcast packets to synchronize their clocks with the information.

The time zone is not set to 8 hours less than Pacific Standard Time. The value -8 in the command clock timezone PST -8 represents the number of hours of offset from UTC time, not from the time zone stated in the clock timezone command.

The router will not listen for NTP broadcasts on the interface E0/0. The ntp broadcast command, when executed under an interface, instructs the router to send NTP broadcast packets on the interface. To set the interface to listen and use NTP broadcasts, you would execute the ntp broadcast client command on the interface.

The router will not periodically update its software clock. The command ntp update-calendar configures the system to update its hardware clock from the software clock at periodic intervals.

Objective:
Infrastructure Services

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

References:
Basic System Management > Setting Time and Calendar Services > Configuring NTP

QUESTION 133
What will an EIGRP router do if the successor route fails and there is no feasible successor?

A. EIGRP will mark the route as passive until a new successor route is determined.
B. EIGRP will redistribute routes into RIP or OSPF.
C. EIGRP will query neighboring routers until a new successor route is determined.
D. EIGRP will forward traffic to the neighbor with the lowest administrative distance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Feasible successors are backup routes for the successor (active) route to a remote network. If a successor route fails, and a feasible successor is available, the feasible successor will immediately become the successor and be installed in the routing table. This provides EIGRP with virtually instantaneous convergence. If no feasible successor is available, then the router must send out query packets to neighboring EIGRP routers to find an alternate path to the remote network.

EIGRP routes are marked as active when the network is converging. Passive routes are stable, converged routes.

EIGRP will not redistribute routes into RIP or OSPF. Redistribution allows information learned from one routing protocol to be converted into routes for injection into the autonomous system of another routing protocol. This allows networks learned via EIGRP, for example, to be visible and reachable from hosts in a RIP routing domain. Redistribution has nothing to do with EIGRP convergence or with the determination of a new successor route.

Administrative distance is used to determine which source of routing information is considered more trustworthy when multiple routing protocols have been implemented. Administrative distance has no effect on EIGRP convergence or the determination of a new successor route.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > Enhanced Interior Gateway Routing Protocol > Document ID: 16406 > Feasible Distance, Reported Distance, and Feasible Successor

QUESTION 134
Examine the output of the show ip route command below:

```
Gateway of last resort is not set

     20.0.0.0/24 is subnetted, 1 subnets
O E2    20.20.20.0 [110/20] via 192.168.1.2, 00:05:10, FastEthernet0/0
O IA 172.16.0.0/16 [50/21] via 192.168.4.1, 00:05:10, FastEthernet0/1
                   [50/21] via 192.168.1.2, 00:05:10, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/32 is subnetted, 1 subnets
C       10.10.10.10 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/20] via 192.168.1.2, 00:05:10, FastEthernet0/0
O    192.168.3.0/24 [110/20] via 192.168.4.1, 00:05:10, FastEthernet0/1
     30.0.0.0/32 is subnetted, 1 subnets
O       30.30.30.30 [50/21] via 192.168.4.1, 00:05:10, FastEthernet0/1
                    [50/21] via 192.168.1.2, 00:05:10, FastEthernet0/0
```

Which of the following statements is FALSE?

A. The route to 30.30.30.30 uses a cost of 21
B. The command ip route 192.168.2.0 255.255.255.0 172.16.14.2 200 will replace the current route to 192.168.2.0/24
C. The route to 192.168.2.0/24 uses the default administrative distance
D. Traffic will be load balanced across two routes to 30.30.30.30

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The command ip route 10.10.10.0 255.255.255.0 172.16.14.2 200 will NOT replace the current route to 10.0.0.0/24.

When you execute the ip route command to enter a static route, the administrative distance can be altered by adding the desired distance value to the end of the command. In this scenario, the administrative distance value was set to 200. The route to the 10.10.10.0/24 network that is currently in the table was learned by OSPF and is using the default administrative distance of 110. Since 110 is lower than 200, the new static route will not be added to the routing table UNLESS the current route becomes unavailable.

The route to 30.30.30.30 does uses a cost of 21, as is indicated by the value on the right side of the forward slash within the brackets found in the route entry, [50/21].

The route to 192.168.2.0/24 uses the default administrative distance. It was learned from OSPF, which has a default distance of 110. Its administrative distance is indicated by the value on the left side of the forward slash within the brackets found in the route entry, [110/20].

Traffic will be load balanced across two routes to 30.30.30.30 because they have equal cost of 21. This cost is indicated by the value on the right side of the forward slash within the brackets found in the route entry, [50/21].

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

References:
Cisco > Support > Cisco IOS IP Routing: Protocol-Independent Command Reference > ip route
Cisco Press > Articles > Cisco Network Technology > General Networking > Cisco Networking Academy's Introduction to Routing Dynamically

QUESTION 135
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:
Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > Route Selection in Cisco Routers

QUESTION 136
What is the purpose of using the show arp command?

A. To view the ARP statistics only for a particular interface
B. To view details regarding neighboring devices discovered by ARP
C. To view global ARP information such as timer and hold time
D. To view the Address Resolution Protocol (ARP) cache

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show arp command is used to view the Address Resolution Protocol (ARP) cache. ARP is used by the Internet Protocol (IP) to find the Media Access Control (MAC) address or the hardware address of a host. The main function of ARP is to translate IP addresses to MAC addresses. The process of obtaining the address of a computer in the network is known as address resolution. This process is accomplished by sending an ARP packet from a source to a destination host. The destination host responds to the ARP packet by replying back to the source and including its own MAC address. Once the source host receives the reply, it will update its ARP cache with the new MAC address. The complete syntax of the show arp command is:

show arp [ip-address [locationnode-id] | hardware-address [locationnode-id] | traffic [locationnode-id | interface-instance] | trace [error [locationnode-id] | dev [locationnode-id] | events [locationnode-id] table [locationnode-id] packets [locationnode-id] | [locationnode-id]] | type instance| [locationnode-id]

The following is a brief description of the parameters used with this command:

ip-address: An optional parameter that displays specific ARP entries.
locationnode-id: An optional parameter that displays the ARP entry for a specific location. The method for entering the node-id argument is rack/slot/module notation.
hardware-address: An optional parameter that displays ARP entries that match the 48-bit MAC address.
traffic: An optional parameter that displays ARP traffic statistics. interface instance:
Either a physical interface instance or a virtual interface instance:

Physical interface instance: the naming notation is rack/slot/module/port and a slash mark between values is required as part of the notation
where: rack refers to the chassis number of the rack. slot refers to the physical slot number of the line card.
module refers to the module number. A physical layer interface module (PLIM) is always 0.
port refers to the physical port number of the interface.
Virtual interface instance: the number range is variable depending on the type of interface.
trace: An optional parameter that displays the ARP entries in the
buffer. error: An optional parameter that displays the ARP error logs.
dev: An optional parameter that displays the ARP internal logs. events:
An optional parameter that displays the ARP events logs. table: An
optional parameter that displays the ARP cache logs.
packets: An optional parameter that displays the ARP packet receive and reply logs. type instance: An
optional parameter that specifies the interface for which you want to view the ARP cache.

An example of the output of the show arp command is shown below along with a diagram of the network in which the router resides.

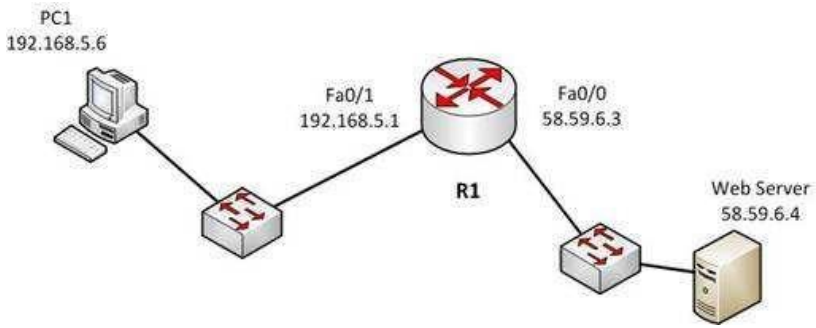
```
R1#show arp
Protocol Address Age (min) Hardware Addr Type Interface
```

```
Internet 192.0.5.1 120 0000.a710.4baf ARPA FastEthernet 0/1

Internet 192.0.5.6 105 0000.a710.859b ARPA FastEthernet 0/1

Internet 58.59.6.3 42 0000.a710.68cd ARPA FastEthernet 0/0

Internet 58.59.6.4 59 0000.0c01.7bbd ARPA FastEthernet 0/0
```



From the information above, we can make the following conclusions about the actions R1 will take when it receives data from PC1 destined for the Web server:

- The data frames will be forwarded out the Fa0/0 interface of R1
- R1 will place the MAC address of the Web Server (0000.0c01.7bbd) in the destination MAC address of the frames
- R1 will put the MAC address if the forwarding Fa0/0 interface (0000.a710.68cd) in the place of the source MAC address

The option stating that the show arp command is used to view the ARP statistics only for a particular interface is incorrect because this command is used to view the ARP cache. You can also view the information for a particular interface with the help of the interface instance parameter.

The options stating that the show arp command is used to view the details of neighboring devices discovered by the ARP or to view global ARP information, such as hold time and timer, are both incorrect because these are both Cisco Discovery protocol (CDP) functions, not ARP functions. The show cdp neighbors detail command is used to display details regarding the neighboring devices that are discovered by CDP, and the show cdp command displays global CDP information, such as timer and hold-time.

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

References:

QUESTION 137
What are the three types of Internet Protocol version 6 (IPv6) addresses? (Choose three.)

A. Unicast
B. Broadcast
C. Dual-cast
D. Anycast
E. Multicast

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Unicast, multicast, and anycast are types of IPv6 addresses.

The following are the IPv6 address types:

- Unicast address: These types of addresses are used to define a single destination interface. A packet sent to a unicast address is delivered to the specific interface.
- Multicast address: These types of addresses are used to define a group of hosts. When a packet is sent to a multicast address, it is delivered to all the hosts identified by that address. Multicast addresses begin with the prefix FF00::/8 and the second octet identifies the range over which the multicast address is propagated. Some special case IPv6 multicast addresses:

  - FF01:0:0:0:0:0:0:1: Indicates all-nodes address for interface-local scope.

  - FF02:0:0:0:0:0:0:2: Indicates all-routers address for link-local.
- Anycast address: These types of addresses are used to identify a set of devices. These addresses are also assigned to more than one interface belonging to different nodes. A packet sent to an anycast address is delivered to just one of the interfaces, based on which one is closest. For example, if an anycast address is assigned to a set of routers, one in India and another in the U.S., the users in the U.S. will be routed to U.S. routers and the users in India will be routed to a server located in India.

The broadcast option is incorrect because these types of addresses are not supported by IPv6. Broadcast functionality is provided by multicast addressing.

The dual-cast option is incorrect because this is not a valid Cisco address type.

Objective:
Network Fundamentals Sub-
Objective:

Compare and contrast IPv6 address types

References:

QUESTION 138
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:
Cisco Documentation > Internetworking Technology Handbook > Ethernet Technologies

QUESTION 139

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:
Infrastructure Management Sub-
Objective:
Configure and verify initial device configuration

References:
Cisco > Cisco IOS Configuration Fundamentals Command Reference > F through K > hostname

QUESTION 140
Which Cisco IOS command can be issued on a router to test the connectivity of one interface from another interface on the same router?

A. ping (with no address specified)
B. ping (with an address specified)
C. tracert
D. traceroute

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The extended ping Cisco IOS utility, which is issued with no address specified, can be issued on a router to test connectivity between two remote routers. The ping utility uses Internet Control Messaging Protocol (ICMP) packets. An ICMP echo request is sent to the destination host. Upon its receipt, the destination host responds to the sending host with an ICMP echo reply. When the echo reply is received, the connectivity is verified. Below is sample output of the extended ping command:

```
Router R#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 12.1.10.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```


The ping command with an address specified is incorrect because you when you issue this command you will either receive a reply from the destination or a destination unreachable message. It will not prompt for additional information as shown which is what allows you to specify the endpoints for the ping.

The traceroute command is not correct for this scenario because this command traces the path between the host issuing the command and the target network.

The tracert command is not a Cisco IOS command, but a Microsoft command.

Objective:

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

References:
Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730 > The Extended ping Command
Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > ping

QUESTION 141
Which of the following statements best describes the result of issuing the command standby 44 timers 3 1 on an HSRP router?

A. The holdtime will be set to a value of 3, and the hellotime will be set to a value of 1.
B. The status of the standby router will be displayed as unknown expired.
C. The role of active router will be passed repeatedly from one router to another.
D. The router will be configured to reassume the role of active router in the event that the router fails and is subsequently restarted.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When the command standby 44 timers 3 1 is issued on a Hot Standby Routing Protocol (HSRP) router, the role of active router will be passed repeatedly from one router to another. This behavior occurs when the timers are set incorrectly. The syntax for the standby timers command is standby [group-number] timers [hellotime holdtime].

The hellotime variable is the number of seconds between hello messages and is set to a value of 3 by default.

The holdtime variable is the number of seconds that the HSRP standby router will wait before assuming that the active router is down; if the standby router believes the active router to be down, it will assume the role of active router.

The holdtime is set to a value of 10 by default. The holdtime should be set to a value at least three times the value of the hellotime. Otherwise, the active router might not be able to respond before the standby router assumes that the active router is down and becomes the new active router.

Because the command standby 44 timers 3 1 sets the hellotime to a value of 3 and the holdtime to a value of 1, the role of active router will be passed from one standby router to the next. To set the holdtime to a value of 3 and the hellotime to a value of 1, the command standby 44 timers 1 3 should be issued. To reset the timer values to their default values, the command no standby group-number timers should be issued.

The status of the standby router will be displayed as unknown expired if a Physical layer problem exists. The unknown expired status can also be displayed if only one HSRP router is configured for the subnet.

To configure an HSRP router to reassume the role of active router in the event that the router fails and is subsequently restarted, the command standby groupnumber preempt should be issued. When the HSRP active router fails or is shut down, the standby router assumes the role of active router. By default, when the original HSRP active router is restarted, it does not take the role of active router away from the original standby router, even if the original active router has a higher priority value. The command standby group-number preempt changes this default behavior.

The holdtime will not be set to a value of 3, and the hellotime will not be set to a value of 1. On the contrary, the hellotime will be set to a value of 3 and the holdtime will be set to a value of 1.

Objective:
Infrastructure Services Sub-
Objective:
Configure, verify, and troubleshoot basic HSRP

References:
Cisco IOS IP Application Services Command Reference > show vrrp through synguard (virtual server) > standby timers
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 142
You have executed the following commands on switch55:


```
switchA(config)# dot1x system-auth-control
switchA(config)# aaa new-model
switchA(config)# radius-server host 192.168.105.67 key firstKey111
switchA(config)# aaa authentication dot1x default group radius
switchA(config)# interface range Fa 0/1 - 11
switchA(config-if)# switchport mode access
switchA(config-if)# dot1x port-control auto
```

What is the result of executing the given commands? (Choose two.)

A. Only the listed RADIUS server is used for authentication
B. 802.1X authentication is enabled on the Fa0/1 interface only
C. The key for the RADIUS server is firstKey111
D. AAA is not enabled on the switch

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

Explanation:
As a result of executing these commands, the default list is used for the RADIUS server for authentication, and the key for the RADIUS server is firstKey111.

A RADIUS server combines the authentication and authorization processes. Before you configure the RADIUS server, you should enable AAA by using the aaa new-model command in global configuration mode. Then, you can specify the location of the RADIUS server and the key using the radius-server host command. In this case, the RADIUS server is located at the IP address 192.168.105.67 and requires the key firstKey111 as the encryption key. This key must be mutually agreed upon by the server and the clients.

The aaa authentication dot1x default group radius command creates a method list for 802.1X authentication. The default group radius keywords specify that the default method will be to use all listed RADIUS servers to authenticate clients. Since only one is listed, it will be the only one used.

It is incorrect to state that 802.1X authentication is enabled only on the Fa0/1 interface. The interface range Fa 0/1 - 11 and the dot1x port-control auto commands specify that 802.1X authentication is enabled on the interfaces Fa0/1 to Fa0/11.

It is incorrect to state that AAA is not enabled on the switch. The aaa new-model command enables AAA globally on the switch.

Objective:
Infrastructure Security Sub-
Objective:
Describe device security using AAA with TACACS+ and RADIUS

References:
Cisco > Support > Cisco IOS Security Command Reference: Commands A to C > aaa new-model
Cisco > Support > Cisco IOS Security Command Reference: Commands D to L > dot1x port-control
Cisco > Support > Cisco IOS Security Command Reference: Commands M to R > radius-server host

QUESTION 143
How many IP addresses are available for hosts in the 192.168.16.64 /26 subnet?

A. 14
B. 30
C. 62
D. 126

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

There are 62 IP addresses available for hosts in the 192.168.16.64 /26 subnet.

The number of host addresses is calculated as 2n - 2, where n is the number of host bits and 2 is subtracted to exclude the network address and the broadcast address.

An IP address has 32 available bits divided into four octets. In the 192.168.16.66 /26 address, the /26 indicates that there are 26 masking bits, or that 26 bits are reserved for the network portion of the address. This leaves 6 bits for the host addresses (32 - 26 = 6).

The following formula is used to calculate the number of IP addresses available for hosts:

Network address: 192.168.16.0
Subnet mask in decimal: 255.255.255.192
Subnet mask in binary: 11111111.11111111.1111111.11000000

Number of bits used for masking = 2^6
Number of hosts bits in the address = 6

Using the formula for calculating the number of hosts per subnet, we find:

Hosts formula: 2number-of-host-bits - 2

Hosts: 2^6 - 2 = 62

For subnet 192.168.16.64, the valid host range starts from 192.168.16.65 and runs to 192.168.16.126. For subnet 192.168.16.128, the valid host range starts from 192.168.16.129 and runs to 192.168.16.190.

The options 14, 30, and 126 are incorrect because 62 IP addresses are available for hosts in the 192.168.16.64/26 subnet.

The correct mask for the size network desired is critical to proper network function. For example, assume a router has an interface Fa0/0 hosting a LAN with 20 computers configured as shown in the following output of show interfaces command:

```
Router# show interfaces
Fastethernet0 is up, line protocol is up
Hardware address is 000b.12bb.4587
Internet address 192.168.10.30/30
```

In this example, the computers will not be able to access anything beyond the LAN because the mask /30 only allows for 2 addresses when 21 (including the router interface) are required.

Objective:

Network Fundamentals Sub-
Objective:
Apply troubleshooting methodologies to resolve problems

References:
Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

QUESTION 144
Refer to the following sample output:

```
GigabitEthernet0/2 is up, line protocol is up
Internet address is 11.1.1.1/16
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN Flow CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is enabled, using route map PBR
Network address translation is disabled
BGP Policy Mapping is disabled
IP Multi-Processor Forwarding is enabled <======== MPF information
IP Input features, "PBR",
are not supported by MPF and are IGNORED
IP Output features, "NetFlow",
are not supported by MPF and are IGNORED
```


Which Cisco Internetwork Operating System (IOS) command produces this output?

A. show interfaces
B. show interfaces summary
C. show ip interface
D. show interfaces serial

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show ip interface command will produce the displayed output. The show ip interface command is used to view the usability status of Internet Protocol (IP) interfaces. The complete syntax of this command is:

show ip interface [type number] [brief]

Following is a brief description of the parameters used in this command:

type: An optional parameter that refers to the type of interface. number: An optional parameter that refers to the interface number. brief: An optional parameter used to view a summarized display of the usability status information for every interface

The show interfaces command does not generate the displayed output. This command is used to view information regarding statistics for specific interfaces.

The show interfaces summary command does not generate the displayed output. This command provides a summarized view of all interfaces configured on a device.

The show interfaces serial command does not generate the displayed output. This command is used to view information for a serial interface.

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

References:

QUESTION 145
You are the network administrator for your company. The Chief Technical Officer of the company is looking for a routing solution that satisfies the following requirements:
- No routing protocol advertisements
- Increased network security
- No routing protocol overhead
- Not concerned about fault tolerance

Which of the following routing techniques matches the criteria?

A. Dynamic routing

B. Hybrid routing
C. Static routing
D. Public routing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The static routing technique matches the criteria given in this scenario. Static routing is a process of manually entering routes into a routing table. Static routes are not recommended for large networks because static routes are manually configured on the router. However, if a single link is used to connect an enterprise to an Internet Service Provider (ISP), then static routing is the best option.

The following are characteristics of static routing:
- Configuring static routes does not create any network traffic.
- Manually configured static routes do not generate routing updates and therefore do not consume any network bandwidth.
- Router resources are used more efficiently.
- Static routes are not recommended for large networks because they are manually configured on the router and maintaining the routes can become problematic.
- Static route configuration is not fault tolerant, because static routes do not automatically adapt to changes in the network.

The dynamic routing option is incorrect because route updates consume bandwidth and overhead. While the scenario is not concerned with routing protocol overhead, it states that there should be no bandwidth consumption by route advertisements.

Hybrid routing and public routing are not valid routing techniques in Cisco terminology.

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

References:
Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Algorithm Types

QUESTION 146
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:

QUESTION 147
You are purchasing a device to upgrade your network. You need to determine the type of device required, as well as the number and type of required interfaces. The device will host three LAN subnets and a T1 Internet connection.

Which of the following device and interface combinations will support this requirement without providing any unnecessary interfaces or using subinterfaces?

A. a switch with one Ethernet interface and three serial interfaces
B. a router with one serial interface and three Ethernet interfaces
C. a router with one serial interface and one Ethernet interface
D. a switch with one modem and three serial interfaces

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This deployment will require a router with one serial interface and three Ethernet interfaces. When LAN subnets and the Internet must be connected, you must deploy a device that can make decisions based on IP addresses. This is the function of a router. Each LAN subnet will require a separate Ethernet interface, and the T1 connection requires a serial interface, so the router must have one serial interface and three Ethernet interfaces.

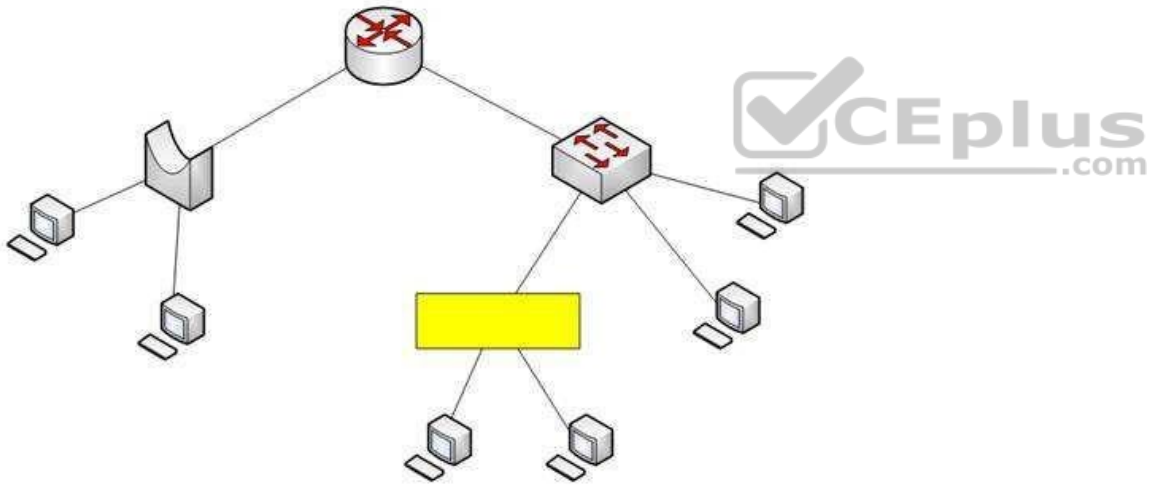
A switch cannot be used to connect separate subnets and the Internet. This requires a router. Switches make forwarding decisions based on MAC addresses. In this deployment, decisions must be made on the basis of IP addresses. Moreover, switches only have Ethernet interfaces, so a switch could not handle the T1 connection.

A router with one serial and one Ethernet interface will not be sufficient. Each LAN subnet will require a separate Ethernet interface.

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

References:
Cisco > Home > Internetworking Technology Handbook > Internetworking Basics > Bridging and Switching Basics

QUESTION 148
Assume that all ports on Layer 2 devices are in the same Virtual LAN (VLAN). View the given network topology. (Click the Exhibit(s) button.)



Which network device should be placed at the highlighted box to produce a total of two broadcast domains and seven collision domains in the network?

A. Hub
B. Bridge
C. Switch
D. Router

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A hub should be placed at the highlighted box to produce a total of two broadcast domains and seven collision domains in the network. Network devices segment collision domains and broadcast domains in the following manner:

- Hub: A Layer 1 device with all ports in same collision domain and broadcast domain.
- Bridge/Switch: Layer 2 devices on which all ports are in different collision domains, but in the same broadcast domain (assuming that all ports are in the same VLAN or no VLAN is configured).
- Routers: A Layer 3 device on which every port is a separate collision as well as broadcast domain.

The bridge shown in the graphic has three ports populated by active links, resulting in three collision domains. The switch shown in the exhibit has four ports populated with the links, resulting in four collision domains. Together these two devices create seven collision domains.
Because the scenario requires that there be no more than seven collision domains, the device in the highlighted box must not create any further collision domains.
A hub is a device that has all its ports in the same collision domain and will not create any further collision domains in the topology.

A bridge or switch cannot be the correct option because these will also add collision domains.

In the exhibit, the router has two ports with active links, which will result into two broadcast domains. Because the scenario states there are no more than two broadcast domains, the device in the highlighted box must not be a router. Routers are used to segment broadcast domains.

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

References:

QUESTION 149
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 generates 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 transport input 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:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Support > Technology Support > Security and VPN > Secure Shell (SSH) > Design > Configuring Secure Shell on Routers and Switches Running Cisco IOS > Document ID: 4145

QUESTION 150
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:
Cisco > Cisco IOS Configuration Fundamentals Command Reference > F through K > hostname

QUESTION 151
Which Wide Area Network (WAN) switching technology is used by Asynchronous Transfer Mode (ATM)?

A. packet switching
B. virtual switching
C. circuit switching
D. cell switching

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Cell switching is a WAN switching technology that is used by ATM. ATM is an International Telecommunication Union-Telecommunications (ITU-T) standard for transmission of data, voice, or video traffic using a fixed size frame of 53 bytes, known as cells. Out of these 53 bytes, the initial five bytes are header information and the rest 48 bytes is the payload.

Packet switching is incorrect because packet switching is popularly used for data transfer, as data is not delay sensitive and it does not require real time transfer from a sender to a receiver. With packet switching, the data is broken into labeled packets and transmitted using packet-switching networks.

Virtual switching is incorrect because no such WAN switching technology exists.

Circuit switching is incorrect because circuit switching dynamically establishes a virtual connection between a source and destination. The virtual connection cannot be used by other callers unless the circuit is released. Circuit switching is the most common technique used by the Public Switched Telephone Network (PSTN) to make phone calls. A dedicated circuit is temporarily established for the duration of call between caller and receiver. Once the caller or receiver hangs up the phone, the circuit is released and is available for other users.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies > Circuit Switching

QUESTION 152
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 2 protocol 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 CDP operates 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.

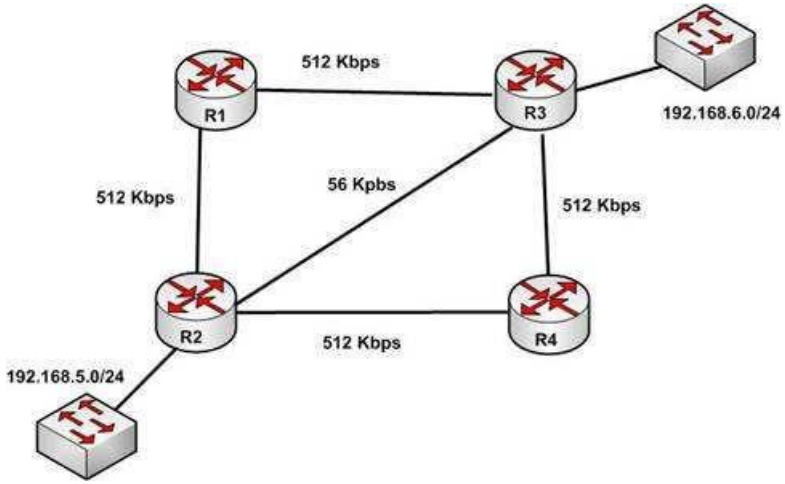
Information is not being passed between the devices through default IP addresses. There is no such thing as default IP addresses on Ethernet interfaces for Cisco routers.

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

References:
Cisco > Cisco IOS Network Management Command Reference > schema through show event manager session cli username > show cdp neighbors

QUESTION 153
With respect to the network shown below, which of the following statements are true when R2 sends a packet to the 192.168.6.0/24 network? (Choose all that apply.)



A. If RIPv1 is in use, the path taken will be R2 - R4 - R3
B. If both RIPv2 and EIGRP are in use, the EIGRP route will be placed in the routing table
C. If EIGRP is in use, the only path taken will be R2 - R4 - R3
D. If RIPv2 is in use, the path taken will be R2 - R3

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If both RIPv2 and EIGRP are in use, the EIGRP route will be placed in the routing table. If RIPv2 is in use, the path taken will be R2 - R3.

EIGRP has a default administrative distance (AD) of 90, while RIPv2 has a default administrative distance (AD) of 120. The route learned by the routing protocol with the lowest AD will be placed in the routing table.

If you wanted to force R2 to use the RIPv2 route instead of the EIGRP route, this could be accomplished by changing the administrative distance of RIPv2 to a value less than 90, such as 80. The commands that would accomplish this are:

```
R2(config)# router rip
R2(config-router)# distance 80
```

If either of the versions of RIP is in use, hop count is used to determine the route. The path with the least number of hops is R2 - R3.

If RIPv1 is in use, the path taken would be R2 - R3, not R2 - R4 - R3, because R2 - R3 has a lower hop count.

If EIGRP is in use, the path R2 - R4 - R3 will not be the only path taken. EIGRP load-balances two equal cost paths when they exist, and R2 - R4 - R3 and R2 - R1 R3 are of equal cost so would both be used.

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast distance vector and link-state routing protocols

References:
Home > Articles > Cisco Certification > CCDA > CCDA Self-Study: RIP, IGRP, and EIGRP Characteristics and Design

QUESTION 154
You are the network administrator for your company. You recently configured Cisco Discovery Protocol (CDP) in the network. You want to view output regarding all of the neighboring devices discovered by CDP. This information should include network address, enabled protocols, and hold time.

Which Cisco Internetwork Operating System (IOS) command would allow you to accomplish this task?

A. show cdp
B. show cdp entry
C. show cdp neighbor entries
D. show cdp neighbors detail

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In this scenario, you should use the show cdp neighbors detail command to view the details of the neighboring devices that were discovered by CDP. CDP is a Layer 2 (data link layer) protocol used to find information about neighboring network devices. The show cdp neighbors detail command is used to view details such as network address, enabled protocols, and hold time. The complete syntax of this command is:

show cdp neighbors [type number] [detail] The

command parameters are defined in this way:

type: An optional parameter which specifies the type of interface used to connect to the neighbors for which you require information.
number: An optional parameter used to specify the interface number connected to the neighbors for which you want information.

detail: An optional parameter used to get detailed information about neighboring devices, such as network address, enabled protocols, software version and hold time.

The following code is a sample partial output of the show cdp neighbors detail command:

```
Device ID: RTR2511
Entry address(es):
IP address: 178.10.20.1
Platform: cisco 2511, Capabilities: Router
Interface Serial 0
Holdtime : 123 sec
<output omitted>

----------------------------------------
Device ID: RTR2611-Edge
Entry address(es):
IP address: 10.10.1.2
Platform: cisco 2611, Capabilities: Router
Interface Ethernet 0
Holdtime : 123 sec
<output omitted>
```

The show cdp command is incorrect because this command is used to view global CDP information such as the timer and hold time.

The show cdp entry command is incorrect because this command is used to view information about a specific neighboring device.

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

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Cisco IOS Network Command Reference, Release 12.4 > show cdp neighbors

QUESTION 155
If a routing table contains multiple routes for the same destination, which were inserted by the following methods, which route will the router use to reach the destination network?

A. The route inserted by RIP
B. The route inserted by OSPF
C. The route inserted by BGP

D. The route configured as a static route

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A static route will be preferred because it has the lowest administrative distance. Routing protocols are dynamic routing methods. With the default configuration, static routes are preferred over dynamic routes.

The default administrative distance for the offered options is:
▪ RIP 120 ▪
OSPF 110 ▪
eBGP 20
▪ Static 1

When Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and static routing is enabled on a router, the router will prefer the static route.

Objective:
Routing Fundamentals Sub-
Objective:
Interpret the components of routing table

References:
Cisco Documentation > Internetworking Technology Handbook > Routing Basics

QUESTION 156
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:
Cisco > Cisco IOS Network Management Command Reference > show cdp interface

QUESTION 157
Which of the following is NOT a mode of Dynamic Trunking Protocol (DTP)?

A. dynamic auto
B. dynamic trunk
C. dynamic desirable
D. nonegotiate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Dynamic trunk is not a DTP mode. DTP is a Cisco proprietary trunk negotiation protocol and is used to determine if two interfaces on connected devices can become a trunk. There are five modes of DTP:

- Trunk: Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.
- Access: Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.
- Dynamic desirable: Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.
- Dynamic auto: Makes the interface willing to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. This is the default mode for all Ethernet interfaces in Cisco IOS.
- Nonegotiate: Puts the interface into permanent trunking mode but prevents the interface from generating DTP frames. You must configure the neighboring interface manually as a trunk interface to establish a trunk link. Use this mode when connecting to a device that does not support DTP.

If one side's mode of link is in trunk mode, dynamic desirable mode, or dynamic auto mode, and the other side is trunk or dynamic desirable, a trunk will form. Nonegotiate mode enables trunking but disables DTP.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:

QUESTION 158
You want to encrypt and transmit data between peer routers with high confidentiality. Which protocol option should you choose?

A. Authentication Header (AH) in tunnel mode
B. Authentication Header (AH) in transport mode
C. Encapsulating Security Payload (ESP) in tunnel mode
D. Encapsulating Security Payload (ESP) in transport mode

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You should choose Encapsulating Security Payload (ESP) in tunnel mode to encrypt and transmit data between peer routers with high confidentiality. Two protocols can be used to build tunnels and protect data traveling across the tunnel:
- Authentication Header (AH) uses protocol 51.
- ESP uses protocol 50.

AH is defined in Request for Comments (RFC) 1826 and 2402. AH does not perform data encryption and therefore, information is passed as clear text. The purpose of AH is to provide data integrity and authentication, and anti-reply service (optional). It ensures that a packet that crosses the tunnel is the same packet that left the peer device and no changes have been made. It uses a keyed hash to accomplish this.

ESP is defined in RFC 2406. ESP can provide data integrity and authentication, but its primary purpose is to encrypt data crossing the tunnel. There are two reasons why ESP is the preferred building block of IPSec tunnels:
- The authentication component of ESP does not include any Layer 3 information. Therefore, this component can work in conjunction with a network using Network Address Translation (NAT).
- On Cisco devices, ESP supports encryption using Advanced Encryption Standard (AES), Data Encryption Standard (DES), or Triple DES (3DES).

Tunnel mode is used between Virtual Private Network (VPN) gateways such as routers, firewalls, and VPN concentrators.

Transport mode is used between end-stations or between an end-station and a VPN gateway.

The options AH in tunnel mode and AH in transport mode are incorrect because AH does not provide encryption.

The option ESP in transport mode is incorrect because transport mode is used between end-stations or between an end-stations and a VPN gateway.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco > Articles > Network Technology > General Networking > IPSec Overview Part Two: Modes and Transforms
Cisco > The Internet Protocol Journal > The Internet Protocol Journal - Volume 3, No. 1, March 2000 > IP Security

QUESTION 159
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 retransmission, 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:
Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Internet Protocols > TCP Packet Format

QUESTION 160
What Cisco Catalyst switch feature can be used to define ports as trusted for DHCP server connections?

A. DHCP snooping
B. port security
C. 802.1x
D. private VLANs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP spoofing is an attack that can be used to force user traffic through an attacking device. This is accomplished by an attacker responding to DHCP queries from users. Eliminating the response from the correct DHCP server would make this more effective, but if the attacker's response gets to the client first, the client will accept it.

The DHCP response from the attacker will include a different gateway or DNS server address. If they define a different gateway, the user traffic will be forced to travel through a device controlled by the attacker. This will allow the attacker to capture traffic and gain company information. If the attacker changes the DNS server in the response, they can use their own DNS server to force traffic to selected hosts to go to a device they control. Again, this would allow the attacker to capture traffic and gain information.

DHCP snooping can be used to determine what ports are able to send DHCP server packets, such as DHCPOFFER, DHCPACK, and DHCPNAK, from the company DHCP server. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

The three required steps to implement DHCP snooping are:
1. Enable DHCP snooping globally with the ip dhcp snooping command:

```
switch(config)# ip dhcp snooping
```

2. Enable DHCP snooping for a VLAN with the vlan parameter:

```
switch(config)# ip dhcp snooping vlan vlan #
    (for example, ip dhcp snooping 10 12 specifies snooping on VLANs 10 and 12)
```

3. Define an interface as a trusted DHCP port with the trust parameter:

```
switch(config-if)# ip dhcp snooping trust
```

When specifying trusted ports, access ports on edge switches should be configured as untrusted, with the exception of any ports that may have company DHCP severs connected. Only ports where DHCP traffic is expected should be trusted. Most certainly, ports in any area of the network where attacks have been detected should be configured as untrusted.

Some additional parameters that can be used with the ip dhcp snooping command are:
- switch(config)# ip dhcp snooping verify mac-address - this command enables DHCP MAC address verification.
- switch(config)# ip dhcp snooping information option allow-untrusted - this command enables untrusted ports to accept incoming DHCP packets with option 82 information. DHCP option 82 is used to identify the location of a DHCP relay agent operating on a subnet remote to the DHCP server.

When DHCP snooping is enabled, no other relay agent-related commands are available. The disabled commands include:

```
ip dhcp relay information check global configuration ip
dhcp relay information policy global configuration ip
dhcp relay information trust-all global configuration ip
dhcp relay information option global configuration ip
dhcp relay information trusted interface configuration
```

Private VLANs are a method of protecting or isolating different devices on the same port and VLAN. A VLAN can be divided into private VLANs, where some devices are able to access other devices and some are completely isolated from others. This was designed so service providers could keep customers on the same port isolated from each other, even if the customers had the same Layer 3 networks.

Port security is a method of only permitting specified MAC addresses access to a switch port. This can be used to define what computer or device can be connected to a port, but not to limit which ports can have DHCP servers connected to them.

802.1x is a method of determining authentication before permitting access to a switch port. This is useful in restricting who can connect to the switch, but it cannot control which ports are permitted to have a DHCP server attached to it.

Objective:
Infrastructure Security Sub-
Objective:
Describe common access layer threat mitigation techniques

References:
Home > Support > Product Support > Switches > Cisco Catalyst 4500 Series Switches > Configure > Configuration Guides > Chapter: Configuring DHCP Snooping and IP Source Guard > Configuring DHCP Snooping on the Switch

QUESTION 161
Examine the partial output from two adjacent routers:

```
RTR78# show ip ospf
Routing Process 201 with ID 192.0.2.1 VRF default
 Stateful High Availability enabled
 Graceful-restart is configured
 Grace period: 60 state: Inactive
 Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an autonomous system boundary
Administrative distance 110
 Reference Bandwidth is 40000 Mbps
 Initial SPF schedule delay 3000.000 msecs,
 minimum inter SPF delay of 2000.000 msecs,
 maximum inter SPF delay of 4000.000 msecs
 Initial LSA generation delay 3000.000 msecs,

RTR79# show ip ospf
Routing Process 202 with ID 192.0.2.1 VRF default
 Stateful High Availability enabled
 Graceful-restart is configured
 Grace period: 60 state: Inactive
 Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an autonomous system boundary
Administrative distance 110
 Reference Bandwidth is 30000 Mbps
 Initial SPF schedule delay 3000.000 msecs,
 minimum inter SPF delay of 2000.000 msecs,
 maximum inter SPF delay of 4000.000 msecs
 Initial LSA generation delay 3000.000 msecs,
```

Which of the following statements describes why the two routers are NOT forming an OSPF neighbor adjacency?

A. The process IDs do not match
B. The router IDs are misconfigured
C. The distance is misconfigured
D. The reference bandwidth does not match

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The output shows that the router IDs for RTR78 and RTR79 are the same value, which should not be the case. One of the two routers has been misconfigured with the other router's ID. This will prevent an OSPF neighbor adjacency from forming.

Other issues can that can prevent an adjacency are:
- Mismatched OSPF area number
- Mismatched OSPF area type
- Mismatched subnet and subnet mask
- Mismatched OSPF HELLO and dead timer values

The process IDs do not have to match. It does not matter whether they match or do not match because the process ID is only locally significant on the device.

The administrative distance is not misconfigured in the output. Both routers are using the default OSPF administrative distance of 110.

If the reference bandwidths do not match, it will affect the calculation of the path cost, but it will not prevent an adjacency from forming.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:
Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > OSPF Neighbor Problems Explained

QUESTION 162
Which of the following is NOT a characteristic of Open Shortest Path First (OSPF)?

A. Is a Cisco-proprietary routing protocol
B. Has a default administrative distance of 110
C. Supports authentication
D. Uses cost as the default metric

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
OSPF is not a Cisco-proprietary routing protocol. It is an industry standard protocol supported by a wide range of vendors. The following are characteristics of OSPF:

- Uses Internet Protocol (IP) protocol 89.
- Has a default administrative distance of 110.
- Is an industry standard protocol (non Cisco-proprietary).
- Supports Non-Broadcast Multi-Access (NBMA) networks such as frame relay, X.25, and Asynchronous Transfer Mode (ATM). The default hello interval for NBMA networks is 30 seconds.
- Supports point-to-point and point-to-multipoint connections.
- Supports authentication.
- Uses 224.0.0.6 as multicast address for ALLDRouters.
- Uses 224.0.0.5 as multicast address for ALLSPFRouters.
- Uses link-state updates and SPF calculation that provides fast convergence.
- Recommended for large networks due to good scalability. ▪

Uses cost as the default metric.

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast interior and exterior routing protocols

References:
Cisco > Articles > Cisco Certification > CCNP > Shooting Trouble with IP
Cisco > Internetworking Technology Handbook > Open Shortest Path First (OSPF)
CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 9: OSPF, pp. 347-361.

QUESTION 163
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 NTP server 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 a client/server mode

References:
Cisco > Support > Product Support > Switches > Cisco Nexus 6000 Series Switches > Configure > Configuration Guides > Cisco Nexus 6000 Series NX-OS System Management Configuration Guide, Release 7.x > Chapter: Configuring NTP

QUESTION 164
You are planning the configuration of an IPsec-protected connection between two routers. You are concerned only with the integrity of the data that passes between the routers. You are less concerned with the confidentiality of the data, and you would like to minimize the effect of IPsec on the data throughput.

Which protocol option should you choose?

A. Authentication Header (AH) in tunnel mode

B. Authentication Header (AH) in transport mode
C. Encapsulating Security Payload (ESP) in tunnel mode
D. Encapsulating Security Payload (ESP) in transport mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
You should choose Authentication Header (AH) in tunnel mode to meet the scenario requirements. Two protocols can be used to build tunnels and protect data traveling across the tunnel:
▪ Authentication Header (AH) uses protocol 51. ▪
ESP uses protocol 50.

AH is defined in Request for Comments (RFC) 1826 and 2402. AH does not perform data encryption, and therefore information is passed as clear text. The purpose of AH is to provide data integrity and authentication, and optionally to provide anti-reply service. It ensures that a packet that crosses the tunnel is the same packet that left the peer device and no changes have been made. It uses a keyed hash to accomplish this.

ESP is defined in RFC 2406. ESP can provide data integrity and authentication, but its primary purpose is to encrypt data crossing the tunnel. On Cisco devices, ESP supports encryption using Advanced Encryption Standard (AES), Data Encryption Standard (DES), or Triple DES (3DES). Tunnel mode is used between Virtual Private Network (VPN) gateways such as routers, firewalls, and VPN concentrators.

You would not choose Authentication Header (AH) in transport mode. Transport mode is used between end stations or between an end station and a VPN gateway.

You would not choose Encapsulating Security Payload (ESP) in tunnel mode or transport mode. Using ESP will slow the connection because of the encryption and decryption process that will occur with each packet.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco > Articles > Network Technology > General Networking > IPsec Overview Part Two: Modes and Transforms
Cisco > The Internet Protocol Journal > The Internet Protocol Journal - Volume 3, No. 1, March 2000 > IP Security
CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 15: Virtual Private Networks, pp. 536-537.

QUESTION 165
Which prompt indicates the configuration mode at which Cisco IOS debug commands can be issued?

A. router>
B. router#
C. router(config)#
D. router(config-if)#

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
You would use privileged EXEC mode, as indicated by the router# prompt, to issue Cisco IOS show and debug commands. All debug commands are entered in privileged EXEC mode. A brief description of all the debugging commands can be displayed by entering the following command in privileged EXEC mode at the command line:

debug?

Debugging output consumes high CPU processing power and can leave the system unusable. The debug commands should be reserved to troubleshoot specific problems, preferably with the help of Cisco technical support staff.

The prompt router> indicates user exec mode, which provides limited access to the router.

The prompt router(config)# indicates global configuration mode, which allows configuration settings affecting the entire router. Passing through this mode is also required to access configuration mode for specific interfaces as well.

The prompt router(config-if)# indicates interface configuration mode, which allows configuration of the interface specified when entering this mode.

Objective:
Infrastructure Management Sub-
Objective:
Configure and verify device management

References:
Cisco > Support > Cisco IOS Software > Using the Command-Line Interface in Cisco IOS Software

QUESTION 166
Refer to the following configuration on a Cisco router to allow Telnet access to remote users:

Router(config)#line vty 0 2
Router(config-line)#login
Router(config-line)#password guest
How many users can Telnet into this router at the same time?

A. 0
B. 1
C. 2

D. 3
E. 5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The given configuration will allow three users to Telnet into the router at the same time. The line vty 0 2 command specifies a range from 0 to 2; therefore, three simultaneous Telnet sessions are allowed on this Cisco router. The commands in the exhibit can be explained as follows:

Router(config)#line vty 0 2 (determines which of the five possible terminal lines are being configured. In this case, they are lines 0 through 2. It also determines the number of lines available, in that any line with no password configured will be unusable.)
Router(config-line)#login (specifies that a password will be required)
Router(config-line)#password guest (specifies the password)

The default configuration allows five simultaneous Telnet sessions on the Cisco router. For the default configuration, you would issue the vty 0 4 command in global configuration mode.

You must configure a password when enabling a router for Telnet access. Without a password, the login access to the router will be disabled and you will receive the following error message if you try to Telnet to the router:

```
router# telnet 10.10.10.1
Trying 10.10.10.1 ... Open
Password required, but none set
[Connection to 10.10.10.1 closed by foreign host]
```

Objective:
Infrastructure Management Sub-
Objective:
Configure and verify device management

References:

QUESTION 167
You are the network administrator for your company. Your company has opened a new site in London. The Chief Technical Officer (CTO) of the company wants to implement a routing protocol that can provide the following features:
- Supports multiple large networks
- Does not require a hierarchical physical topology

- Supports VLSM
- Provides loop prevention and fast convergence
- Provides load balancing over un-equal cost links

Which routing protocol should be implemented in the new site?

A. Enhanced Interior Gateway Routing Protocol (EIGRP)
B. Open Shortest Path First (OSPF)
C. Interior Gateway Routing Protocol (IGRP)
D. Routing Information Protocol version 2 (RIPv2)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Enhanced Interior Gateway Routing Protocol (EIGRP) is the routing protocol that should be implemented for this scenario. EIGRP is a classless protocol that allows the use of variable length subnet masks (VLSM) and classless interdomain routing (CIDR) for the allocation of IP addresses. The following are characteristics of EIGRP:

- Supports large networks due to high scalability.
- Does not require a hierarchical physical topology.
- Provides loop prevention and fast convergence by using Diffusing Update Algorithm (DUAL).
- Performs equal cost load balancing by default.
- Can be configured to perform unequal-cost load balancing.
- Supports VLSM and CIDR.
- Is a hybrid routing protocol (a distance-vector protocol that also provides link-state protocol characteristics). ▪

Is a classless protocol.

- Sends partial route updates only when there are changes.
- Supports Message-Digest algorithm 5 (MD5) authentication.
- Has an administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes. ▪

Is only used with Cisco platforms.

All the other options are incorrect because they would not provide the features required in this scenario.

OSPF requires a hierarchical physical topology.

IGRP does not support VLSM.

RIPV2 is not designed for multiple large networks.

Objective: Routing
Fundamentals Sub-
Objective:
Compare and contrast distance vector and link-state routing protocols

References:
Cisco > Articles > Cisco Certification > CCNP > Shooting Trouble with IP
Cisco > Support > IP > IP Routing > Design > Design TechNotes > Introduction to EIGRP > Document ID: 13669

QUESTION 168
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.

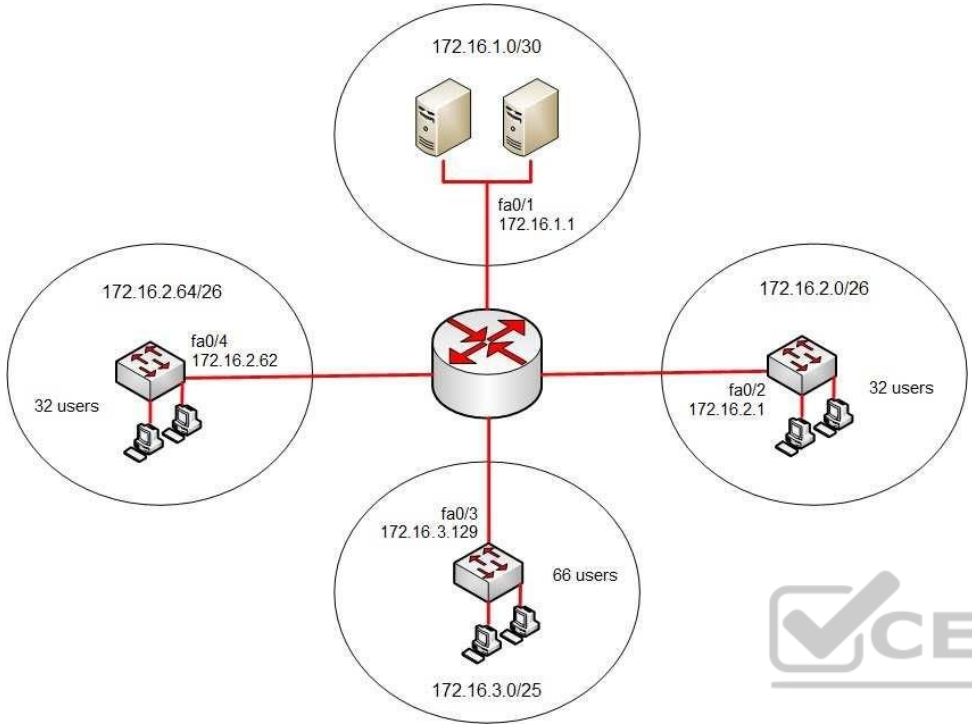
Fa0/3 is not a trunk port. It only carries traffic from VLAN 1.

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

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

References:

QUESTION 169
Your company's network must make the most efficient use of the IP address space. In the following diagram, the circles define separate network segments. The requirements of each network segment are given in the diagram. (Click the Exhibit(s) button.)



Users complain of connectivity issues. You need to discover the problems with the network configuration.

What are the three problems with the network diagram? (Choose three.)

A. The 172.16.1.0/30 segment requires more user address space.
B. The 172.16.2.0/26 segment requires more user address space.
C. The 172.16.3.0/25 segment requires more user address space.
D. The 172.16.2.64/26 segment requires more user address space.
E. Interface fa0/2 has an IP address that belongs to the 172.16.2.64/26 segment.
F. Interface fa0/4 has an IP address that belongs to the 172.16.2.0/26 segment.
G. Interface fa0/3 has an IP address outside the 172.16.3.0/25 segment.

Correct Answer: AFG

Section: (none)
Explanation
Explanation/Reference:
Explanation:
The given exhibit has three problems:
- The 172.16.1.0/30 segment requires more user address space.
- Interface Fa0/4 has an IP address that belongs to the 172.16.2.0/26 segment.
- Interface Fa0/3 has an IP address outside the 172.16.3.0/25 segment.

The 172.16.1.0/30 segment, as configured, will only support two hosts. This segment needs to support three hosts, the two servers, and the Fa0/1 interface. The number of hosts that a subnet is capable of supporting is a function of the number of host bits in the subnet mask. When that has been determined, the following formula can be used to determine the number of hosts yielded by the mask:

2n - 2 = X
(where n = the number of host bits in the mask and X = the number of hosts supported)

In this example with a 30-bit mask, 2 host bits are left in the mask. When that is plugged into the formula, it yields only two usable addresses. The -2 in the formula represents the two addresses in each subnet that cannot be assigned to hosts, the network ID and the broadcast address. Therefore, the segment should be configured with the 172.16.1.0/29 address range, which supports up to six hosts.

Interface fa0/4, as configured, has an IP address that belongs to the 172.16.2.0/26 segment. With a 26-bit mask and the chosen class B address, the following network IDs are created:

172.16.0.0
172.16.0.64
172.16.1.128
172.16.1.192
172.16.2.0
172.16.2.64
172.16.2.128
172.16.2.192
172.16.2.0
172.16.2.64
172.16.2.128
172.16.2.192
...and so on, incrementing each time by 64 in the last octet

The 172.16.2.0/26 segment is allocated host addresses in the 172.16.2.1 through 172.16.2.62 range (the last address, 172.16.2.63, is the broadcast address and cannot be assigned). Interface fa0/4 should be assigned an IP address in the 172.16.2.64/26 range, which includes host addresses in the 172.16.2.65 through 172.16.2.126 range.

Interface Fa0/3, as configured, has an IP address outside the 172.16.3.0/25 segment. With a 25-bit mask and the chosen class B address, the following network IDs are created:

172.16.0.0
172.16.0 141
172.16.1.0 141
172.16.1 224
172.16.2 224
172.16.3.0 224
172.16.3...and so on, incrementing each time by 128 in the last octet ..... **Error! Bookmark not defined.**

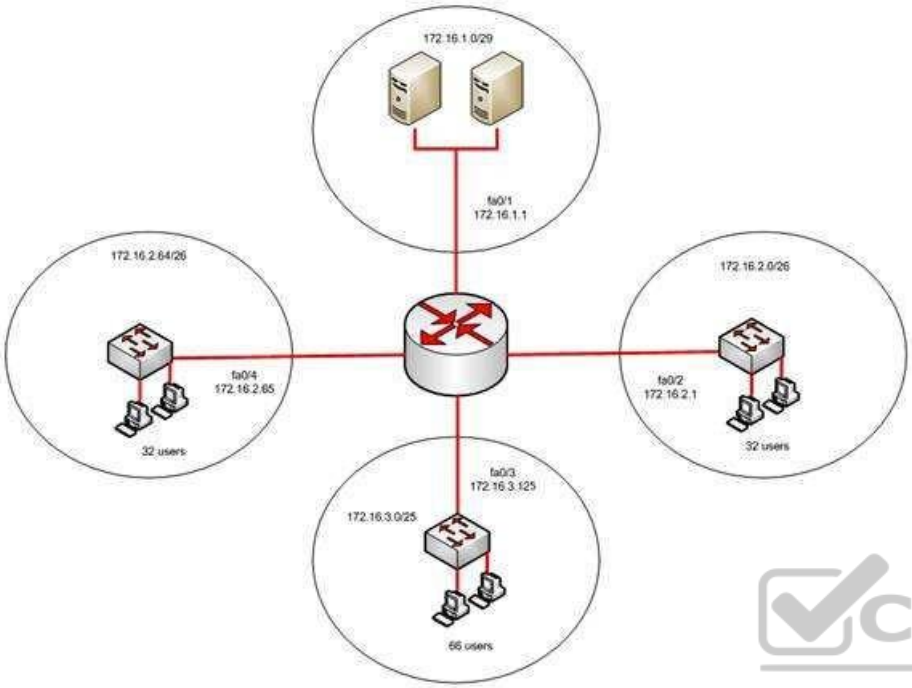
172.16.2.0
Interface Fa0/3 should be allocated an IP address in the 172.16.3.1 through 172.16.3.126 range.

The 172.16.2.0/26 segment does not require more user address space. With a 26-bit mask, 6 bits are left for hosts, and by using the above formula it can be determined that it will yield 62 hosts. It requires 32.

The 172.16.2.64/26 segment does not require more user address space. With a 26-bit mask, 6 bits are left for hosts, and by using the above formula it can be determined that it will yield 62 hosts. It requires 32.

Interface Fa0/2 does not have an IP address that belongs to the 172.16.2.64/26 segment. The 172.16.2.64/26 segment includes addresses 172.16.2.65172.16.5.126. Because its address is 172.16.2.1, it belongs in the 172.16.2.0/26 network (from 172.16.2.1-172.16.2.62), so it is correctly configured.

The network should be configured as shown in the following image:



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

References:
IP Addressing and Subnetting for New Users

QUESTION 170
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:
Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

QUESTION 171
Which of the following are classless routing protocols? (Choose four.)

A. Open Shortest Path First (OSPF)

B. Enhanced Interior Gateway Routing Protocol (EIGRP)
C. Interior Gateway Routing Protocol (IGRP)

D. Routing Information Protocol version 1 (RIPv1) E. Border Gateway Protocol (BGP)
F. Routing Information Protocol version 2 (RIPv2)

Correct Answer: ABEF
Section: (none)
Explanation

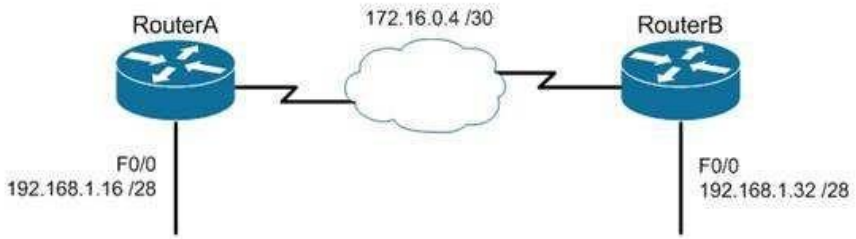
Explanation/Reference:
Explanation:
Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), and Routing Information Protocol version 2 (RIPv2) are classless routing protocols.

Intermediate-System-to-Intermediate System (IS-IS) is also a classless routing protocol.

The options IGRP and RIPv1 are incorrect because these are classful routing protocols.

The following are characteristics of classless routing protocols:
- The subnet mask is advertised with each route by using classless routing protocols.
- Flexible route summarization and supernetting (CIDR) are allowed in classless routing protocols.
- Classless routing protocols support variable length subnet masks (VLSM), which allow different subnets of a given IP network to be configured with different subnet masks.

One of the main advantages of using a classless routing protocol is its ability to minimize the effects of discontiguous networks. When subnets of the same classful network are separated by another classful network, the networks are called discontiguous. Examine the diagram below:



The LAN networks extending from Router A and Router B are derived from the same Class C network, 192.168.1.0/24. A classful routing protocol such as RIP v1 would not be able to determine the direction to send the packets, but since classless protocols include the subnet mask in advertisements, they would not suffer the same problem. Whenever networks with non-default subnet masks are used, a classless routing protocol will be required.

Below are some examples of networks that do not have default masks. You can recognize them by the fact that they are not /8, /16, or /24.

192.168.10.0/27
10.5.6.0/22
172.68.0.0/18

All of the classless protocols discussed here are interior routing protocols with the exception of Border Gateway Protocol (BGP), which is an external routing protocol used to connect different autonomous systems. For example, BGP would be used to connect two OSPF autonomous systems (AS).

Objective:
Routing Fundamentals Sub-
Objective:
Interpret the components of routing table

References:
Cisco > Support > IP > IP Routing

QUESTION 172
You are configuring a serial link between a Cisco router and a router produced by another vendor. What would be the advantages of using Point to Point Protocol (PPP) over High Level Data Link Control (HDLC) in this scenario?

A. HDLC has a proprietary "type" field that may be incompatible with equipment from other vendors.

B. HDLC is not available on non-Cisco routers.
C. PPP is faster.
D. PPP performs error checking.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
High Level Data Link Control (HDLC) has a proprietary "type" field that may be incompatible with equipment from other vendors. It is recommended that PPP always be used when combining equipment from multiple vendors because this Data Link layer WAN protocol is an industry standard. PPP is implemented in the same manner on all PPP-capable equipment.

HDLC is available on non-Cisco routers. However, the Cisco implementation has a "type" field that may prevent the connection from working.

PPP is not faster than HDLC.

PPP performs error checking, but so does HDLC.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco > Internetworking Technology Handbook > Point to Point Protocol (PPP)

QUESTION 173
Which WAN switching technology is used with ISDN?

A. packet switching
B. virtual switching
C. circuit switching
D. cell switching

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Circuit switching dynamically establishes a connection between a source and a destination. The connection cannot be used by other callers until the circuit is released. Circuit switching is the most common technique used with the public switched telephone network (PSTN) to make phone calls. During a call, a dedicated virtual circuit is temporarily established between the caller and receiver for the duration of the call. Once the caller or receiver hangs up the phone, the circuit is released and is made available for other users.

Packet switching is a technique popularly used for transfer of data that is not delay sensitive and does not require real-time transfer rates from a sender to a receiver. Also unlike circuit switching which makes a fixed amount of bandwidth available for the connection (which may not be fully utilized) packet switching uses bandwidth more efficiently. With packet switching, the data is broken into labeled packets and is transmitted using packet-switching networks.

Cell switching is used by Asynchronous Transfer Mode (ATM). ATM is an International Telecommunication Union-Telecommunications (ITU-T) standard for transmission of data, voice, or video traffic using a fixed size frame of 53 bytes, known as cells. Of these 53 bytes, the initial five bytes are header information and the remaining 48 bytes are the payload. These cells are transmitted over a path that may vary with each cell. It does not maintain a dedicated virtual circuit.

The term "virtual switching" is incorrect because it is not a valid WAN switching technology.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:
Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies > Circuit Switching

QUESTION 174
Which of the following are NOT valid IPv6 addresses? (Choose all that apply.)

A. 225.1.4.2 B.
::FFFF:10.2.4.1
C. ::
D. 2001:0:42:3:ff::1
E. fe80:2030:31:24
F. 2001:42:4:0:0:1:34:0
G. 2003:dead:bef:4dad:ab33:46:abab:62

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The addresses 255.1.4.2 and fe80:2030:31:24 are not valid IPv6 addresses.

225.1.4.2 is incorrect because it is an IPv4 multicast address. The address fe80:2030:31:24 is incorrect because it does not represent a 16-byte IPv6 address, with colons separating each 2-byte segment.

IPv6 addresses are 16 bytes, or 128 bits in length. The following are valid IPv6 addresses.

- ::FFFF:10.2.4.1 is an example of an IPv4-compatible IPv6 address, where the first 10 bytes (80 bits) of the address are set to 0 the next 2 bytes (16 bits) are set to FFFF and the last 32 bits are the IPv4 address
- :: is the IPv6 "unspecified address." It is a unicast address not assigned to any interface, and is used by a DHCP-dependent host prior to allocating a real IPv6 address.
- 2001:0:42:3:ff::1 is a valid IP address, with the :: representing two segments (4 bytes) of compressed zeros.
- 2001:42:4:0:0:1:34:0 is a valid IP address, with only the leading zeros of each segment truncated.
- 2003:dead:beef:4dad:ab33:46:abab:62 has 16 bytes, is divided correctly by colons into eight sections, utilizes the dropping of leading zeros in each section correctly, and uses the letters a-f in the three section that spell out dead beef 4 dad.

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast IPv6 address types

References:
Cisco > Technology Support > IP > IPv6 > Technology Information > Technology White Paper > IPv6 Addressing At A Glance (PDF)
Cisco > Internetworking Technology Handbook > IPv6

QUESTION 175
The conference room has a switch port available for use by the presenter during classes. You would like to 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:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot port security

References:
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA>Configuring Port Security

QUESTION 176
Given the following output, which statements can be determined to be true? (Choose three.)

```
RouterA2# show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
192.168.23.2 1 FULL/BDR 00:00:29 10.24.4.2 FastEthernet1/0
192.168.45.2 2 FULL/BDR 00:00:24 10.1.0.5 FastEthernet0/0
192.168.85.1 1 FULL/- 00:00:33 10.6.4.10 Serial0/1
192.168.90.3 1 FULL/DR 00:00:32 10.5.5.2 FastEthernet0/1
192.168.67.3 1 FULL/DR 00:00:20 10.4.9.20 FastEthernet0/2
```

```
192.168.90.1 1 FULL/BDR 00:00:23 10.5.5.4 FastEthernet0/1
<<output omitted>>
```

A. This router is the DR for subnet 10.1.0.0.
B. The DR for the network connected to Fa0/0 has an interface priority greater than 2.
C. The DR for the network connected to Fa0/1 has a router ID of 10.5.5.2.
D. The DR for the serial subnet is 192.168.85.1.
E. This router is neither the DR nor the BDR for the Fa0/1 subnet.
F. RouterA2 is connected to more than one multi-access network.

Correct Answer: BEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show ip ospf neighbor command displays a list of all OSPF routers with which you have established a neighbor relationship. The following describes the command output:
▪ Neighbor ID: the Router ID (RID) of the neighboring router

▪ Pri: the interface priority of the neighboring router, which is used to determine which router should serve the function of a Designated Router (DR) ▪
State: the functional state of the neighboring router
▪ Dead Time: the period that the router will wait to hear a Hello packet from this neighbor before declaring the neighbor down ▪
Address: the IP address of the neighboring router on this subnet
▪ Interface: the local interface over which the neighbor relationship (adjacency) was formed

The output for neighbor 192.168.45.2 is as follows:

192.168.45.2 2 FULL/BDR 00:00:24 10.1.0.5 FastEthernet0/0

This indicates that the interface priority of neighbor 192.168.45.2 is 2. The default OSPF interface priority is 1, and the highest interface priority determines the designated router (DR) for a subnet. This same line reveals that this neighbor is currently the backup designated router (BDR) for this segment, which indicates that another router became the DR. It can be then be assumed that the DR router has an interface priority higher than 2. (The router serving the DR function is not present in the truncated sample output.)
The output for the two neighbors discovered on F0/1 is as follows:

192.168.90.3 1 FULL/DR 00:00:32 10.5.5.2 FastEthernet0/1
192.168.90.1 1 FULL/BDR 00:00:23 10.5.5.4 FastEthernet0/1

This output indicates that router 192.168.90.3 is the DR, and router 192.168.90.1 is the BDR for this network. Since there can only be one DR and BDR per segment, this indicates that the local router is neither the DR nor the BDR. (OSPF considers these DROther routers.)

The fact that multiple DRs are listed in this output indicates that RouterA2 is connected to more than one multi-access segment, since each segment will elect a DR.

It cannot be determined if this router is the DR for subnet 10.1.0.0. The output indicates that router 192.168.45.2 is the BDR for this network, but with the truncated output, it cannot be determined if this router is the DR.

The DR for the network connected to Fa0/1 does not have a router ID of 10.5.5.2. The Address field of the show ip ospf neighbor command indicates the IP address of the neighbor's interface, not the router ID of the neighbor.

The DR for the serial subnet is not 192.168.85.1, since point-to-point serial interfaces do not elect DRs and BDRs. This is indicated by the output below:

192.168.85.1 1 FULL/- 00:00:33 10.6.4.10 Serial0/1

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:
Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039 > DR Election

QUESTION 177
Which statement is supported by the following output?

```
router# show ip protocols
Routing Protocol is "eigrp 3"
Sending updates every 90 seconds, next due in 24 seconds
<<some output omitted>>
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 3
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
172.160.72.0
192.168.14.0
```

```
<<output omitted>>
```

A. EIGRP supports load-balancing over three equal-cost paths
B. EIGRP supports load-balancing over three unequal-cost paths
C. EIGRP supports load-balancing over four equal-cost paths
D. EIGRP supports load-balancing over four unequal-cost paths

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Maximum path: 4 output indicates that Enhanced Interior Gateway Routing Protocol (EIGRP) will support round-robin load-balancing over four equal-cost paths. This is a default setting, and is a true statement for most routing protocols (including RIP, OSPF and IS-IS). Equal-cost paths are different routes to the same destination network with identical metrics, as determined by the routing protocol. Most routing protocols allow this maximum to be raised up to 16 with the maximum-paths command.

EIGRP has the additional benefit of allowing unequal cost load-balancing. With unequal cost load-balancing, the router can be configured to include less desirable (higher-metric) paths in the routing table. The router will then send a balanced percentage of traffic over both the best route and the less desirable paths, such as sending two packets over the best path plus one over a less desirable path. EIGRP will never perform unequal-cost load-balancing by default; it must be configured with a variance command. Therefore, you cannot state that EIGRP supports load-balancing over unequal-cost paths in this example.

You cannot state that EIGRP will support load-balancing over three paths because the output displays the Maximum path: 4 value.

Objective:

Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > IP > IP Routing > Design > Design TechNotes > How Does Load Balancing Work? > Document ID: 5212
Cisco > Support > IP > IP Routing > Design > Design TechNotes > How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP? > Document ID: 13677

QUESTION 178
You have two routers in your OSPF area 0. Router 1 is connected to Router 2 via its Serial 1 interface, and to your ISP via the Serial 0 interface. Router 1 is an ASBR.

After your assistant configures a default route on Router 1, you discover that whenever either router receives packets destined for networks that are not in the routing tables, it causes traffic loops between the two routers.

To troubleshoot, you execute the show run command on Router 1. Part of the output is shown below:

```
<output omitted>
IP route 0.0.0.0 0.0.0.0 serial 1
Router ospf 1
Network 192.168.5.0 0.0.0.255 area 0 Default-
information originate
```

Which command or set of commands should you execute on Router 1 to stop the looping traffic while maintaining Router 2's ability to send traffic to the Internet?

A. Execute the no default-information originate command.
B. Execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command and then execute the ip route 0.0.0.0 0.0.0.0 serial 0 command.
C. Execute the default-information originate always command.
D. Execute the no network 192.168.5.0 area 0 command and then execute the network 192.168.5.0 255.255.255.0 area 0 command.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command followed by the ip route 0.0.0.0 0.0.0.0 serial 0 command. The original configuration command was executed on the wrong interface on Router 1 by your assistant. It should be executed on Serial 0, which is the connection to the ISP. The show run command indicates that with the current configuration, if Router 2 receives a packet not in its table, it sends it to Router 1, and then Router 1 sends it back out on Serial 1. This redirects the packet back to Router 2, and the loop begins. By changing the configuration to Serial 0, Router 1 will start forwarding all traffic not in the routing table to the ISP.

You should not execute the no default-information originate command. This command instructs Router 1 to NOT inject the default route into area 0, which is the desired behavior. Running this command would stop the loop, but would leave Router2 with no default route to send packets to the Internet.

You should not execute the default-information originate always command. It will not change the existing looping behavior. The addition of the always parameter instructs Router 1 to inject a default route into area 0, even if one does not exist on Router 1. This is unnecessary, since Router 1 does have a default route configured, and will not change the existing looping behavior. To advertise a default route to other OSPF routers, you should run this command:

Router1(config-router)#default information originate

You should not execute the no network 192.168.5.0 area 0 command followed by the network 192.168.5.0 255.255.255.0 area 0 command. There is nothing wrong with the original network command. Also, the network 192.168.5.0 255.255.255.0 area 0 command uses an incorrect mask type. The mask must be in the wildcard format. Moreover, since it is incorrect, this will have the effect of disabling OSPF on the network connecting the two routers.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:
Cisco > Home > Support > Technology Support > IP > IP Routing > Configure > Configurations Examples and Technotes > How OSPF Injects a Default Route into a Normal Area

QUESTION 179
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 errorfree 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:
Cisco Documentation > Internetworking Case Studies > LAN Switching

QUESTION 180
Which type of Dynamic Host Configuration Protocol (DHCP) transmission is used by a host to forward a DHCPDISCOVER packet to locate a DHCP server on the network?

A. unicast
B. broadcast
C. multicast
D. anycast

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Hosts broadcast DHCPDISCOVER messages to locate a DHCP server. The following steps are followed during the allocation of the IP address dynamically using a DHCP server:
- The client device broadcasts a DHCPDISCOVER message to locate a DHCP server.
- The DHCP server replies with a DHCPOFFER unicast message with configuration parameters, such as an IP address, a MAC address, a domain name, and a lease for the IP address for the client device.
- The client returns a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the DHCP server.
- The DHCP server replies to client device with DHCPACK unicast message, acknowledging the allocation of the IP address to this client device.

Dynamic Host Configuration Protocol (DHCP) is an enhancement over Bootstrap Protocol (BOOTP) and is used to automate the distribution of IP address to clients from a central server. BOOTP protocol was also used to distribute IP addresses, but was inflexible to changes in the network.

DHCP offers the following three advantages that 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

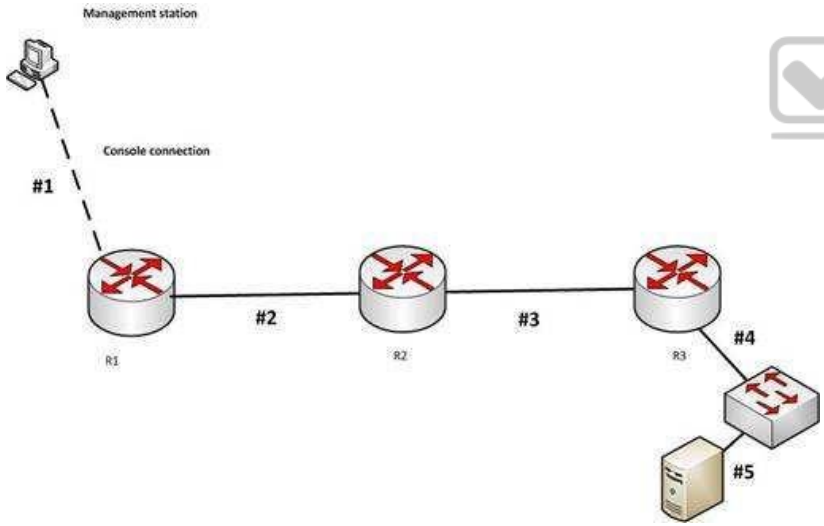
DHCP does not use multicast messages.

Anycast is a concept of IPv6 protocol and is not valid type used by DHCP.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify DHCP on a router (excluding static reservations)

References:
Cisco > Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 > Part 3: DHCP > DHCP Server, Relay Agent, and Client Operation

QUESTION 181
You need to cable the network shown below.



Which of the following is the correct cable for each numbered link?

A. 1-crossover, 2-staight-through, 3-rollover, 4- crossover, 5-crossover
B. 1-straight-through, 2-staight-through, 3-rollover, 4- crossover, 5-crossover

C. 1-crossover, 2-crossover, 3-rollover, 4- crossover, 5-crossover
D. 1-rollover, 2-crossover, 3-crossover, 4- straight-through, 5-straight through

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The correct cabling pattern is 1-rollover, 2-crossover, 3-crossover, 4- straight-through, 5-straight through. When selecting cables, the following rules apply: ▪ Router to router- crossover
▪ Router to switch- straight- through
▪ Management station (PC) to router for console session- rolled cable
▪ Switch to switch - crossover
▪ PC to switch- straight through

Objective:
Network Fundamentals Sub-
Objective:

Select the appropriate cabling type based on implementation requirements

References:
Cisco > Product Support > End-of-Sale and End-of-Life Products > Cisco 7000 Series Routers > Troubleshooting TechNotes > Cabling Guide for Console and AUX Ports > Document ID: 12223

QUESTION 182
Examine the partial output of the show ip interface command below.

```
Router# show ip interface

Serial0 is up, line protocol is up
Internet address is 1.1.1.2/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set

GigabitEthernet0/3 is up, line protocol is up
Internet address is 192.168.93.1/28
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
```


What is the subnet broadcast address of the LAN connected to the router from which the command was executed?

A. 192.168.93.15
B. 192.168.93.255
C. 1.1.1.255
D. 1.1.1.127

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:
In the output we can see there are two interfaces, a serial interface (which goes to another router) and a GigabitEthernet interface (the LAN interface). The LAN interface has an address of 192.168.93.1/28, which is a mask of 255.255.255.240. When this mask is used against the 192.168.93.0 classful network, it yields the following subnets:

192.168.93.0
192.168.93.16

192.168.93.32 192.168.93.48 and so on, incrementing in
intervals of 16 in the last octet.

Since the LAN interface has an address of 192.168.93.1, the interface is in the 192.168.93.0/28 network. That networks broadcast address is the last address before the next subnet address of 192.168.93.16. Therefore, the broadcast address of the LAN connected to the router from which the command was executed is 192.168.93.15.

The address 192.168.93.255 is not the broadcast address. If a standard 24-bit mask were used instead of the /28, this would be the broadcast address.

The address 1.1.1.255 is the broadcast address of the network in which the Serial interface resides. The question asked for the LAN interface.

The address 1.1.1.127 would be the broadcast address of the network in which the Serial interface resides if the mask used on the interface were 255.255.255.128. However, that is not the mask, and the question asked for the LAN interface.

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

References:

QUESTION 183
Which Cisco command will display the version and configuration data for Secure Shell (SSH)?

A. show ssh
B. show ip ssh

C. debug ssh
D. debug ip ssh

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show ip ssh command is used to display the version and configuration data for SSH on a Cisco router. The following is sample output of the show ip ssh command:

```
router#show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 2
```

This show ip ssh command output displays the enabled status of the SSH protocol, the retries parameter (configured at two attempts), and the timeout of 120 seconds.

The following message will appear when the show ip ssh command is issued and SSH has been disabled:

```
router# show ip ssh
%SSH has not been enabled
```

To enable SSH include the transport input SSH command when configuring authentication on a line. For example, the configuration of a Cisco network device to use SSH on incoming communications via the virtual terminal ports, with a specified password as shown from the partial output of the show run command is shown below:

```
line vty 0 4 password 7
030752180500 login
transport input ssh
```

It is important to note the login command on the third line of the above ouput is critical for security. This command instructs the device to prompt for a username and password using SSH. If this line reads no login, SSH might be otherwise be correctly configured, but the device will never prompt for the username and password.

The show ssh command will display the status of the SSH connections on the router The following is the sample output of the show ssh command:

```
router# show ssh
Connection Version Encryption      State              Username
     0     1.5     3DES           Session Started          tim
```

The debug ip ssh command is used to display debug messages for SSH.

The debug ssh command is not a valid Cisco command.

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

References:
Cisco > Cisco IOS Security Command Reference > show ip ssh

QUESTION 184
You are the senior network administrator for a large corporation. Some new trainees have recently joined the network security team. You are educating them about denial-of-service (DoS) attacks and the risks posed to a network by such attacks.

Which three are risks that a DoS attack poses to a network? (Choose three.)

A. Downtime and productivity loss
B. Spread of viruses
C. Revenue loss
D. Information theft
E. Spread of spyware

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A DoS attack can result in network downtime and loss of productivity, revenue loss, and information theft.

A DoS attack is an attack in which legitimate users are denied access to networks, systems, or resources. The potential risks posed by a DoS attack are as follows:
- Downtime and productivity loss: A DoS attack causes downtime in the network, which ultimately results in loss of productivity for the organization.
- Revenue loss: Organizations that use their Web sites for commerce or vital support services, such as search engines, can incur large revenue losses.
- Information theft: DoS attacks can also be aimed at stealing important and confidential information from a network.
- Malicious competition: An organization might launch DoS attacks against their competitors to damage their reputation.

A few methods that can help minimize potential risks from DoS attacks are:
- Using a firewall, which allows you to block or permit traffic entering into the network, can help to mitigate DoS attacks.
- Computers 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.

A DoS attack does not result in the spread of viruses because viruses are not spread by DoS attacks. Viruses are spread when the network is attacked by a virus or a Trojan horse.

A DoS attack does not result in the spread of spyware. DoS attacks are mainly aimed at exhausting system resources so that legitimate users are denied access to networks, systems, or resources. Spyware is software installed on a computer without the knowledge of the user, and it gathers information about a person or organization. Spyware is generally downloaded through Web sites and e-mail messages.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Cisco IOS Security Configuration Guide, Release 12.4 > Traffic Filtering, Firewalls, and Virus Detection > Configuring TCP Intercept (Preventing Denial-ofService Attacks)

QUESTION 185
Which of the following methods of tunneling Internet Protocol version 6 (IPv6) traffic through an IPv4 network increases protocol overhead because of IPv6 headers?

A. Protocol translation
B. IPv6 over dedicated WAN links
C. Dual-Stack Backbones
D. IPv6 over IPv4 tunnels

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
IPv6 over IPv4 tunnels is a method of tunneling IPv6 traffic through an IPv4 network that eliminates the need to create separate circuits to connect to the IPv6 networks. This model increases protocol overhead because of IPv6 headers.

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

- IPv6 over IPv4 tunnels: IPv6 traffic is encapsulated into IPv4 packets. Then these packets are transferred over 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 both ends to be capable of both protocols.

- Protocol translation: A method 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:
Cisco > Technology Support > IP > IPv6 > Configure > Configuration Examples and TechNotes > Tunneling IPv6 through an IPv4 Network > Document ID: 25156

QUESTION 186
Which of the following statements is NOT true of Cisco ACI?

A. It is a comprehensive SDN architecture.
B. It uses Cisco APIC as the central management system.
C. It provides policy driven automation support.
D. It decreases network visibility.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Cisco ACI does not decrease network visibility. On the contrary, the Cisco Application Centric Infrastructure (ACI) increases network visibility. It is a policydriven automaton solution that can keep the network inventory up-to-date automatically whenever a new device is added and provide a graphic representation at all times.

ACI is a comprehensive SDN architecture that integrates physical and virtual environments under one policy model. It uses the Cisco Application Policy Infrastructure Controller (APIC) as the central management system.

It provides policy driven automation support through a business-relevant application policy language.

Objective:
Infrastructure Management

Sub-Objective:
Describe network programmability in enterprise network architecture

References:
Home > Support > Product Support > Cloud and Systems Management > Cisco Application Policy Infrastructure Controller (APIC) > Reference Guides > Technical References Cisco Application Centric Infrastructure Fundamentals

QUESTION 187
Your assistant has been assigned the task of configuring one end of a WAN link between two offices. The link is a serial connection and the router on the other end is a non-Cisco router. The router in the other office has an IP address of 192.168.8.6/24. The connection will not come up, so you ask your assistant to show you the commands he configured on the Cisco router. The commands he executed are shown below.

Ciscorouter(config)# interface serial0/0
Ciscorouter(config-if)# ip address 192.168.8.5 255.255.255.0 Ciscorouter(config-if)# no shut

What command(s) should he run to correct the configuration?

A. Ciscorouter(config-if)# no ip address 192.168.8.5
Ciscorouter(config-if)# ip address 192.168.8.10 B.
Ciscorouter(config-if)# encapsulation ppp
C. Ciscorouter(config-if)# encapsulation ansi
D. Ciscorouter(config-if)# authentication chap

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are three encapsulation types available for a serial connection: High-Level Data Link Control (HDLC), Point-To-Point (PPP), and Frame Relay. HDLC is the default on Cisco routers and the form of HDLC used on a Cisco router is incompatible with routers from other vendors. Since the encapsulation command was not

run, the router is set for HDLC. To correct this, you should execute the encapsulation ppp command. Frame Relay could also be used if the other router were running Frame Relay, since it also is an industry standard.

The IP address does not need to be changed. It is currently set for 192.168.8.5/24. This is correct since it is in the same subnet as the IP address of the other end,192.168.8.6/24.

The command authentication chap should not be run because the scenario does not indicate that authentication is configured on the other end. If it is set on one end, it must be set on the other as well.

The command encapsulation ansi should not be run because ANSI is not an encapsulation type. It is an LMI type used in Frame Relay. The three LMI options available are Cisco, ANSI, and ITU.

Objective: WAN
Technologies Sub-
Objective:
Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

QUESTION 188
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 Address Autoconfiguration (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:
Cisco > Support > IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3S > Chapter: IPv6 Access Services: Stateless DHCPv6

QUESTION 189
You are the network administrator for your company and have configured Cisco Discovery Protocol (CDP) in your network. You recently noticed that when devices send large numbers of CDP neighbor announcements, some devices are crashing. You decide to disable CDP on the router.

Which command should you use to achieve the objective?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should use the no cdp run command to disable CDP on the router. Due to a known vulnerability regarding the handling of CDP by Cisco routers and switches when devices send large numbers of CDP neighbor announcements, some devices can crash or cause abnormal system behavior. To overcome this problem, you can disable CDP for the entire router by using the no cdp run command.

You cannot use the set cdp disable command to disable CDP on the router. This command disables CDP on an entire Catalyst switch.

You cannot use the no cdp enable command to disable CDP on the router. This command disables CDP on a specific interface.

You cannot use the no cdp advertise-v2 command to disable CDP on the router. This command disables CDPv2 advertisements.

Objective:

LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Support > Using Cisco Discovery Protocol
Cisco > Support > Technology Support > Network Management > Cisco's Response to the CDP Issue > Document ID: 13621

QUESTION 190
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.

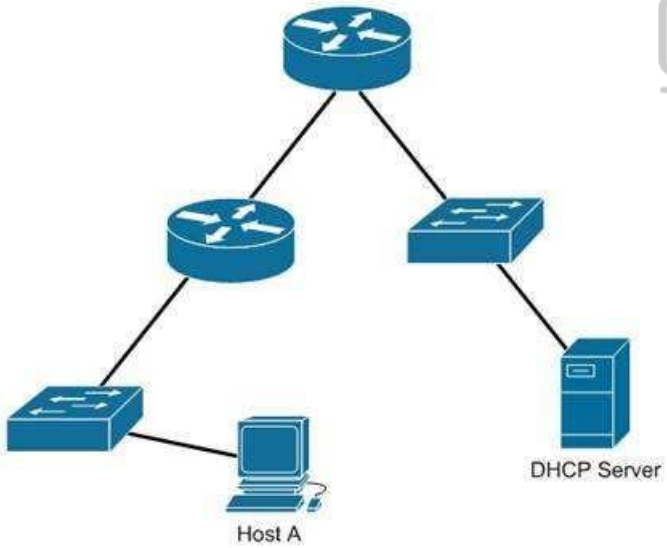
Flow control is incorrect because flow control is used to prevent the loss of traffic between two devices.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Support > Technology Support > Security and VPN > Authentication Protocols > Technology Information > Technology White Paper > Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks > Document ID: 13634

QUESTION 191
Host A is configured for DHCP, but it is not receiving an IP address when it powers up.

What is the most likely cause? (Click the Exhibit(s) button to view the network diagram.)



A. The DHCP server is on the wrong subnet.
B. Routers do not forward broadcast traffic.
C. The DHCP server is misconfigured.
D. Port security is enabled on the switch.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Host A is not receiving a DHCP configuration because its initial DHCP Discover frame is a broadcast, and routers do not forward broadcast frames by default.

A DHCP client sends out a DHCP Discover packet when booting up, enveloped within an Ethernet broadcast frame. The broadcast frame will be flooded by switches, but filtered by routers. There must either be a DHCP server on the local subnet or a DHCP Relay Agent, which will forward the request from the local subnet to the DHCP server.

The DHCP server is not on the wrong subnet. A DHCP server can be centrally located and configured to support multiple remote subnets, as long as those subnets have DHCP Relay Agents configured to forward the DHCP Discover requests.

No information is provided on the DHCP server configuration. The router is the most obvious cause of the problem, so this option is incorrect.

Port security can be configured to restrict hosts based on the MAC address, but the scenario does not provide information on any port security configurations. The router is the most obvious cause of the problem as shown in the network exhibit.

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify DHCP on a router (excluding static reservations)

References:
Cisco > Support > Cisco IOS Software > Configuring the Cisco IOS DHCP Server
Cisco > Support > Cisco IOS Software > Configuring the Cisco IOS DHCP Relay Agent

QUESTION 192
Which VLAN can NOT be filtered through the VLAN Trunking Protocol (VTP) Pruning feature of Cisco switches?

A. VLAN 1
B. VLAN 10

C. VLAN 100
D. VLAN 1000

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
VLAN 1 traffic cannot be pruned. Cisco recommends that VLAN 1 be used for management of VLANs.

VTP pruning is a Cisco VTP feature that allows switches to dynamically delete or add VLANs to a trunk for traffic transmission. It creates an efficient switching network by optimal use of available trunk bandwidth.

The options 10, 100, and 1000 are incorrect because these VLAN numbers can be pruned. By default, VLANs 2 to 1000 are eligible for pruning.

Objective:

LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco Press Home > Articles > Cisco Certification > CCNA > CCNA Self-Study (ICND Exam): Extending Switched Networks with Virtual LANs

QUESTION 193
Which Cisco Internetwork Operating System (IOS) command is used to encrypt passwords on Cisco routers?

A. password secure
B. service encryption-password
C. service password-encryption
D. enable password

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The service password-encryption command is used to encrypt passwords on Cisco routers. It is used to encrypt all passwords configured on the router, both current and future. This means all passwords in the plain text configuration file will be encrypted. This command is issued in global configuration mode. The syntax of the command is as follows:

Router(config)# service password-encryption

This command does not have any parameters.

Once executed any password in the configuration file will appear similar to what is shown below when the running or startup configuration files are viewed:

```
R1#show run <output
omitted> line console 0
password 7 09-4f60C0B1C1B
login
<output omitted>
```

The password secure and service encryption-password commands are incorrect because they are not valid Cisco IOS commands.

The enable password command is used to set the privileged EXEC mode password, and does not encrypt the password by default.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Cisco IOS Security Configuration Guide, Release 12.4 > Part 7: Secure Infrastructure > Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

QUESTION 194
A new security policy has been adopted by your company. One of its requirements is that only one host is permitted to attach dynamically to each switch port. The security settings on all of the ports have been altered from the default settings.

You execute the following command on all switch ports of Switch A:

```
SwitchA(config-if)# switchport port-security maximum 1
```

After executing the command, you discover that users in the Sales department are still successfully plugging a hub into a port and then plugging two or three laptops into the hub.

What did you do wrong?

A. The command should be executed at the global prompt.
B. The command should be executed as switchport port-security maximum 0.
C. You also need to execute the switchport port-security violation shutdown command at the global prompt.
D. You also need to execute the switchport port-security violation shutdown command on each switch port.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When configuring switch port security to enforce the policy described in the scenario, two commands are required. One command specifies how many addresses are allowed per switch port and the other tells the switch what to do when a violation occurs. Configuring the first without the second is like creating a rule without enforcing the rule. Both commands must be executed on each switch port, as shown in the following example:

```
switchA(config)# interface fa0/22 switchA(config-if)#
switchport port-security maximum 1 switchA(config-if)#
switchport port-security violation shutdown
```

By default, ports are configured to shut down on a violation, but the scenario states the default settings have been altered.

The switchport port-security violation command can be set to shutdown, restrict, or protect. The shutdown option shuts down the port if there is a security violation, but does not send an SNMP trap logging the violation. The restrict option drops all packets from insecure hosts at the port-security process level and increments the security-violation count, and can send an SNMP trap. The protect option drops all the packets from the insecure hosts at the port-security process level, but does not increment the security-violation count or send an SNMP trap.

You should not execute either the switchport port-security violation command or the switchport port-security maximum command at the global prompt. Both commands must be executed on each switch port.

You should not execute the command switchport port-security maximum 0. This would tell the switch to not allow any addresses at all per switch port.

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

References:
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport port-security maximum

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport port-security violation

QUESTION 195
Which service is denoted by TCP/UDP port number 53?

A. Domain Name Service (DNS)
B. File Transfer Protocol (FTP)
C. Telnet
D. HTTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port number 53 is assigned to Domain Name Service (DNS), which is used to convert hostnames into Internet Protocol (IP) addresses.

Some common TCP and UDP port number assignments are as follows:
▪ port 25: Assigned to Simple Mail Transfer Protocol (SMTP), a TCP protocol used to send and receive e-mail messages. ▪
port 23: Assigned to Telnet to allow remote logins and command execution.

▪ port 21: Assigned to File Transfer Protocol (FTP). It is used to control FTP transmissions. Port number 20 is also used by FTP for FTP data. ▪
port 80: Assigned to Hypertext Transfer Protocol (HTTP), which is the base for transferring Web pages over the Internet.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering

References:
Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems>Multiplexing Basics

QUESTION 196
You are configuring a Cisco router.

Which command would you use to convey a message regarding the remote access security policy of your organization to a user logging into the router?

A. hostname

B. banner motd
C. description
D. boot system
E. terminal monitor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 and is generally used to communicate routers identification information, display any warning specific to the router, or display a remote access security policy, such as "Unauthorized access to the router is prohibited." The syntax for this command is as follows: **banner motd [d message d]**

d is the delimiter character. It can be any character of the administrator's choice, with the limitation that the delimiter character cannot be used in the message text.

The hostname command is a global configuration command to assign the router a name for identification. The command syntax is hostname [name].

The description command is an interface configuration mode command that sets a description for that interface.

The boot system command is used to specify the path to the primary IOS file. It is a global configuration command.

The terminal monitor command is used to direct debug and system error message to the monitor when connected to a router using telnet. When you are connected to a router using telnet and you issue the debug command, by default the output can only have been seen through a console session with that router. Executing the terminal monitor command directs that output to the terminal session where it can be viewed.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Cisco IOS Configuration Fundamentals Command Reference > F through K > banner motd

QUESTION 197
What switch security configuration requires AAA to be configured on the switch?

A. VACL

B. 802.1x
C. Private VLAN
D. port security

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
802.1x requires AAA to be configured on the switch. 802.1x uses AAA authentication to control access to the port.

The overall steps required to configure a switch for 802.1x are:
- Enable AAA on the switch.
- Define the external RADIUS server(s) and the key to be used for encryption.
- Define the authentication method.
- Enable 802.1x on the switch.
- Configure each switch port that will use 802.1x.
- Optionally allow multiple hosts on the switch port.

Objective:
Infrastructure Security Sub-
Objective:
Describe device security using AAA with TACACS+ and RADIUS

References:
Consolidated Platform Configuration Guide, Cisco IOS XE Release 3E (Cisco 5700 Series WLC) - Configuring IEEE 802.1x Port-Based Authentication (PDF)

QUESTION 198
Which statement is TRUE regarding the switchport protected interface configuration command and its effects?

A. The command is used to configure private VLAN edge ports.
B. The command enables the highest level switch port security.
C. All the traffic through protected port should go via a Layer 2 device such as switch.
D. A protected port can directly communicate with any other port on the same switch.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The switchport protected interface configuration command is used to configure private VLAN edge ports on a Cisco Catalyst 2950 switch. A VLAN edge port is another name given to a protected port. Protected ports do not forward any traffic to other protected ports on the same switch. All traffic passing between protected ports on the same switch must be routed through a Layer 3 device. Protected ports have no restrictions on forwarding to non-protected ports, and they forward as usual to all ports on other switches

Following are the steps to configure a switch port as a protected port:

1. configure terminal
2. interface interface-id
3. switchport protected
4. end

Use the show interfaces switchport command to verify that the protected port is enabled.

It is incorrect to state that the command enables the highest level of switch port security. It places no additional restrictions on the port other than preventing it from directly forwarding from one protected port to another.

It is incorrect to state that all traffic through protected port should go via a Layer 2 device such as a switch. Traffic through the protected port should go via a Layer 3 device, such as a router.

It is incorrect to state that a protected port can directly communicate with any other port on the same switch. A protected port cannot directly communicate with another protected port on the same switch.

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

References:
Cisco > Catalyst 2960 Switch Command Reference, 12.2(44)SE > Catalyst 2960 Switch Cisco IOS Commands - shutdown through vtp > switchport protected

QUESTION 199
Which Cisco IOS interface configuration command is used to configure the private VLAN edge ports on a Cisco Catalyst 2950 switch?

A. switchport protected
B. switchport port-security
C. switchport port-vlan-edge
D. switchport port-security violation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The switchport protected interface configuration command is used to configure protected ports (private VLAN edge ports) on a Cisco Catalyst 2950 switch. A protected port cannot directly communicate with any other protected port on the same switch. It is used in cases where an application requires that no traffic be directly passed from port to port on the same switch. All traffic through the protected port must be transmitted via a Layer 3 device, such as a router.

The switchport port-security command enables basic switch port security. With this command, you can define a group of source MAC addresses (called an address table) that are allowed to access the port. The switch will not forward any packets to the port with source addresses that do not match this group. This is one method a network administrator can use to prevent unauthorized access to the LAN by only allowing company-known MAC addresses. Controlling which MAC addresses can access a port has the following advantages:

- It can ensure full bandwidth on the port if the table is limited to a single source address.
- It can make the port more secure by preventing access from unknown MAC addresses. It can also be used to prevent access on unused ports to prevent unauthorized hosts from accessing the LAN.

The switchport port-security violation command further defines actions a switch can take on the interface in the event of a security violation by following the command with a choice from the {shutdown | restrict | protect} options.

The switchport port-vlan-edge command is incorrect because this is not a valid Cisco command.

Objective:
Infrastructure Security

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

References:

QUESTION 200
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 Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > Part 1: Cisco IOS User Interfaces Commands > Connection, Menu, and System Banner Commands > banner login

QUESTION 201
What will be the effect of executing the following command on port F0/1?

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

A. The command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port.
B. The command expressly prohibits the MAC address of 00c0.35F0.8301 as an allowed host on the switch port.
C. The command configures an inbound access control list on port F0/1 limiting traffic to the IP address of the host.
D. The command encrypts all traffic on the port from the MAC address of 00c0.35F0.8301.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port. 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 violation policies (such as disabling the port) if additional hosts try to gain a connection.

The switchport port-security mac-address 00C0.35F0.8301 command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port.

The switchport port-security mac-address 00C0.35F0.8301 command does not expressly prohibit the MAC address of 00c0.35F0.8301 as an allowed host on the switch port. The port-security command is designed to identify allowed MAC addresses not prohibited addresses.

The switchport port-security mac-address 00C0.35F0.8301 command does not configure an inbound access control list on port F0/1 limiting traffic to the IP address of the host. It will accept traffic to the port, but will only allow a device with that MAC address to be connected to the port.

The switchport port-security mac-address 00C0.35F0.8301 command does not encrypt all traffic on the port from the MAC address of 00c0.35F0.8301. The portsecurity command has nothing to do with encryption.

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

References:
Cisco > Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide > Configuring Port Security > Enabling Port Security
Cisco > Support > Cisco IOS Security Command Reference: Commands S to Z > switchport port-security mac-address

QUESTION 202
What command disables 802.1x authentication on a port and permits traffic without authentication?

A. dot1x port-control disable
B. dot1x port-control force-unauthorized
C. dot1x port-control auto
D. dot1x port-control force-authorized

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The command dot1x port-control force-authorized is used to disable 802.1x on a port and permit traffic without authentication. Dot1x ports are in one of two states, authorized or unauthorized. Authorized ports permit user traffic to flow through the port. This state usually follows successful authentication. Unauthorized ports only permit authorization traffic to flow through the port.

Usually a port begins in the unauthorized state. A user is then allowed to exchange AAA authentication traffic with the port. Once the user has been authenticated successfully, the port is changed to the authorized state and the user is permitted to use the port normally.

Normal use of 802.1x has the port configured with the dot1x port-control auto statement. This places the port in the unauthorized state until successful authentication. After successful authentication, the port is changed to the authorized state.

When 802.1x is initially configured, the default port control of the ports is force-authorized. This forces the port to be in the authorized state without successful authentication. This setting disables the need for authentication and permits all traffic.

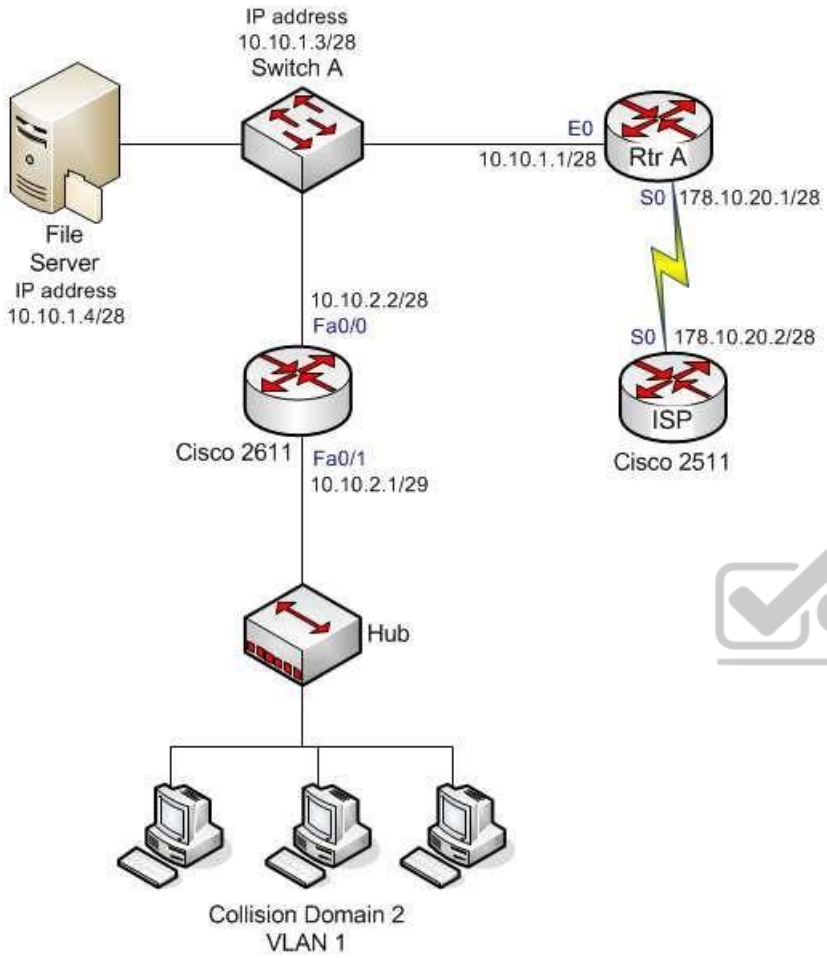
The force-unauthorized keyword configures the port as an unauthorized port regardless of authentication traffic. A port configured with this key word would not permit user traffic, not even authentication traffic.

The command dot1x port-control disable is not a valid command due to incorrect syntax.

Objective:
Infrastructure Security Sub-
Objective:
Describe device security using AAA with TACACS+ and RADIUS

References:
Cisco > Catalyst 6500 Series Release 15.0SY Software Configuration Guide > Security > IEEE 802.1X Port-Based Authentication
Cisco > Support > Cisco IOS Security Command Reference: Commands D to L > dot1x port-control

QUESTION 203
What will be the output of the show cdp neighbors detail command issued on Router A? (Click the Exhibit(s) button to view the network diagram.)



A. Device ID:
RTR2511Entry
address(es):
IP address: 178.10.20.1
Platform: cisco 2511, Capabilities: Router
Interface Serial 0

Device ID: RTR2611-Edge

Entry address(es):
IP address: 10.10.1.2
Platform: cisco 2611, Capabilities: Router
Interface Ethernet 0

B. Device ID:
RTR2611Entry
address(es):
IP address: 172.10.20.1
Platform: cisco 2611, Capabilities: Router
Interface Ethernet 0

Device ID: C2924C-123
Entry address(es):
IP address: 10.10.1.3
Platform: cisco WS-C2924, Capabilities: Switch
Interface Ethernet 0

C. Device ID:
RTR2511Entry
address(es):
IP address: 178.10.20.2
Platform: cisco 2511, Capabilities: Router
Interface Serial 0

Device ID: C2924C-123
Entry address(es):
IP address: 10.10.1.3
Platform: cisco WS-C2924, Capabilities: Switch
Interface Ethernet 0

D. Device ID:
RTR2611Entry
address(es):
IP address: 172.10.20.1
Platform: cisco 2611, Capabilities: Router
Interface Ethernet 0

E. Device ID: C2924C-
123Entry address(es):

IP address: 10.10.1.3
Platform: cisco WS-C2924, Capabilities: Switch
Interface Ethernet 0

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:
The following code is the correct partial output of the show cdp neighbors detail command issued on Router A:

Device ID: RTR2511
Entry address(es):
IP address: 178.10.20.2
Platform: cisco 2511, Capabilities: Router
Interface Serial 0

Device ID: C2924C-123
Entry address(es):
IP address: 10.10.1.3
Platform: cisco WS-C2924, Capabilities: Switch
Interface Ethernet 0

The show cdp neighbors detail command displays the Cisco devices directly connected to the router. Therefore, only details of the 2511 router and the Cisco Catalyst 2924 switch will be displayed in the output. The detail keyword in the show cdp neighbor command also displays IP address information for the directly connected devices. The output shows the connected device name, its IP address, its platform, and the local interface through which the device is connected.

All of the other code samples are incorrect, as they include the output of devices that are not connected directly to Router A.

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol used by all Cisco devices to collect information about neighboring devices. CDP operates at Layer 2 of the OSI model. Therefore, it can collect information about neighboring devices that are running different Network layer protocols. It is also useful for collecting information when IP is not functional.

Some variations of this command include:
- The show cdp command, which displays global CDP information, including timer and hold time information.
- The show cdp interface command, which displays information about the interfaces on which CDP is enabled.
- The show cdp neighbors command, which displays detailed information about neighboring devices discovered by the CDP. However, it does not include the IP address of the neighboring device.

Objective:

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

References:
Cisco > Cisco IOS Network Command Reference, Release 12.4 > show cdp neighbors

QUESTION 204
Which of the following technologies should be used to prevent a switching loop if a switch is connected to a port configured for PortFast?

A. RSTP
B. BPDU Guard
C. Root Guard
D. PVST

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
BPDU Guard prevents switching loops in the case of a switch being connected to a PortFast interface. PortFast is used for ports that connect to host systems, such as workstations and printers, and allows the port to immediately enter a forwarding state. This bypasses the normal 30-second delay that Spanning Tree Protocol would normally use to determine if a switch has been connected to the port. Implementing BPDU Guard will disable the port if a switch is connected and a BPDU is received.

Rapid Spanning Tree Protocol (RSTP) is incorrect because this is an enhanced Spanning Tree standard that operates on the Data Link layer of the OSI model. RSTP was not designed to protect PortFast ports. PortFast and BPDU Guard are supported by RSTP, but they not required or configured by default.

Root Guard is incorrect because it is used to protect the root bridge placement in the Spanning Tree, not to protect PortFast ports.

Per-VLAN Spanning Tree (PVST) is incorrect because this is an implementation of Spanning Tree (the default protocol for Cisco switches), and was not designed to protect PortFast ports. PortFast and BPDU Guard are supported by RSTP, but are not required, and must be configured manually.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP-related optional features

References:

Cisco > Support > Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, and LoopGuard > Understanding How PortFast Works
CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot STP protocols

QUESTION 205
Which of the following cables would be used to connect a router to a switch?

A. v.35
B. crossover
C. rollover

D. straight-through

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A straight-through cable would be used. When connecting "unlike" devices, such as a switch to a router, a straight-through cable is used. This is a cable where the wires are in the same sequence at both ends of the cable.

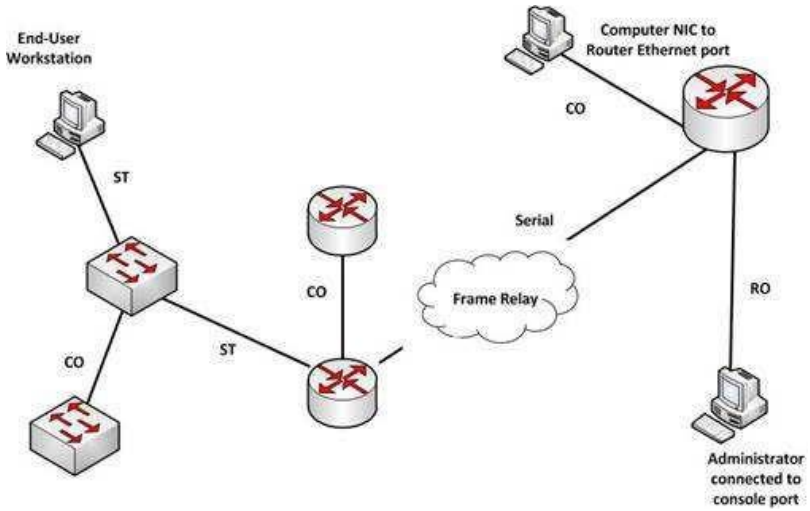
NOTE: The one exception to this general rule of connecting unlike devices with a straight-through cable is when a computer NIC is connected to an Ethernet port on a router. In that case, a crossover cable is used.

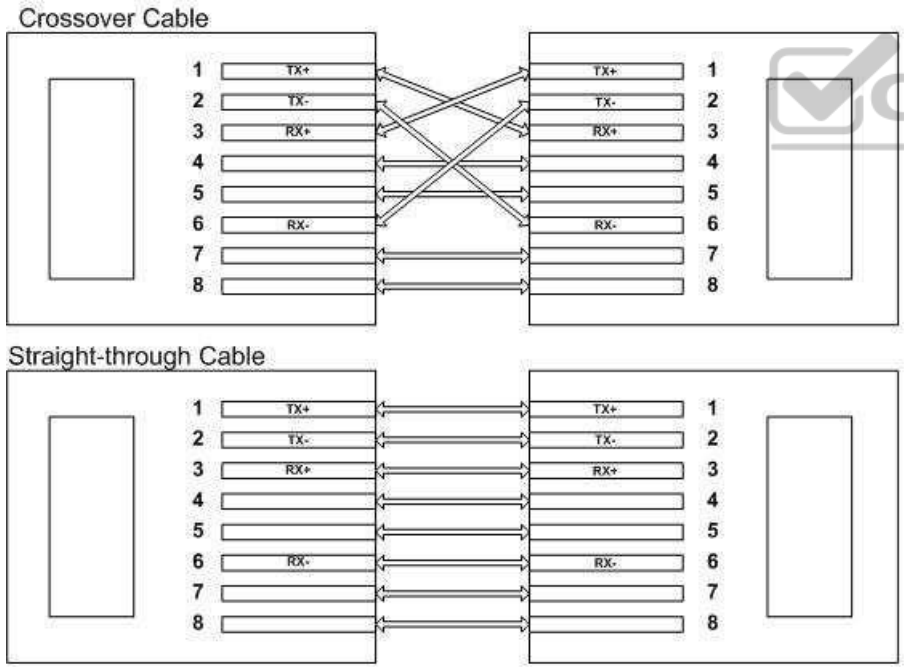
A v.35 cable is used to connect serial connections between routers. This cable has a male DB-60 connector on the Cisco end and a male Winchester connector on the network end. It comes in two types: DCE and DTE. It is often used to simulate a WAN connection in lab environments. In that case, the DCE end acts as the CSU/DSU and is the end where the clock rate is set. A CSU/DSU (Channel Service Unit/Data Service Unit) is a device that connects the router to the T1 or T3 line.

A crossover cable has two wires reversed and is used to connect "like" devices, such as a switch to a switch. It is also used when a computer NIC is connected to an Ethernet port on a router.

A rollover cable is used to connect to the console port of a router to configure the router. It is also called a console cable.

The diagram below illustrates the correct usage of each of the cable types shown using the following legend: ▪
SO Ethernet Straight through Cable
▪ CO Ethernet Crossover Cable
▪ Serial Serial cable
▪ RO Rollover cable





RX = Receive, TX = Transmit

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

References:
Cisco > Product Support > Routers > Cisco 1000 Series Routers > 5-in-1 V.35 Assembly and Pinouts > Document ID: 46803
Cisco > Tech Notes > Cabling Guide for Console and AUX Ports > Document ID: 12223

QUESTION 206
Which metric does the Open Shortest Path First (OSPF) routing protocol use for optimal path calculation?

A. MTU
B. Cost
C. Delay
D. Hop count

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
OSPF is a link-state routing protocol which uses cost as a metric for optimal path calculation. It is an open standard protocol based on Dijkstra's Shortest Path First (SPF) algorithm. Metrics are used by routing protocols to determine the lowest cost path to a network number, which is considered the optimal or "fastest" path. Cisco's implementation of OSPF calculates the cost (metric) of a link as inversely proportional to the bandwidth of that interface. Therefore, a higher bandwidth indicates a lower cost, and a more favorable metric.

For this to work properly, the bandwidth of the link must be configured to allow OSPF to arrive at the cost of the link. This is done with the bandwidth command executed in interface configuration mode, and is entered in kbps. For example, if the link were 64 kbps, you would enter the following command:

```
Router(config-if)# bandwidth 64
```

The metric for any OSPF link defaults to 100,000,000/bandwidth. The bandwidth used in the formula is in bits per second. So, in this example the calculation would be 100,000,000 / 64000 = 1562.5. The cost assigned to the link would be 1562. The cost for a network route is the sum of all individual links in the path to that network.

If multiple paths are assigned equal costs, OSPF will load balance across the multiple paths. By default, it will limit this load balance to a maximum of four equalcost paths. When this occurs, all four equal-cost paths will be placed in the routing table. There are two approaches to allow or prevent load balancing when multiple equal cost paths are available:

- Use the bandwidth command to make one or more of the paths either less or more desirable.
- Use the ip ospf cost command to change the cost value assigned to one or more of the paths

Maximum Transmission Unit (MTU), bandwidth, delay, load, and reliability form a composite metric used by Interior Gateway Routing Protocol (IGRP) and Enhanced Interior Gateway Routing Protocol (EIGRP). IGRP is a distance vector routing protocol developed by Cisco Systems. Enhanced IGRP (EIGRP) is a Cisco-proprietary hybrid protocol having features of both distance-vector and link-state protocols.

Hop count is a metric used by Routing Information Protocol (RIP). The fewer hops between the routers, the better the path.

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast distance vector and link-state routing protocols

References:
Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039
Cisco > Internetworking Technology Handbook > Open Shortest Path First (OSPF)

QUESTION 207
Which commands would be used to enable Enhanced Interior Gateway Routing Protocol (EIGRP) on a router, and configure the IP addresses 10.2.2.2 and 192.168.1.1 as a part of complete EIGRP configuration? (Choose three.)

A. router eigrp 10
B. router eigrp
C. network 10.2.2.2
D. network 10.0.0.0
E. network 192.168.1.0
F. network 192.168.1.1

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The router eigrp 10 command is used to enable EIGRP on a router. The network 10.0.0.0 and network 192.168.1.0 commands are used to activate EIGRP over the interfaces configured with IP addresses 10.2.2.2 and 192.168.1.1. If we were given the subnet mask for the two interfaces, we could include that in the network command as well.

The following command sequence is used to configure EIGRP on a router:

router(config) # router eigrp [autonomous-system]
router (config-router) # network x.x.x.x [wildcard-mask]
router (config-router) # network y.y.y.y [wildcard-mask]

The autonomous-system parameter of the router eigrp command specifies the autonomous system number. To ensure that all the routers in a network can communicate with each other, you should specify the same autonomous system number on all the routers.

The parameters of the network command are:
- x.x.x.x - This is the major (classful) network number connected to the router.
- y.y.y.y - This is the other major (classful) network number connected to the router.

If either the AS numbers do not match between two EIGRP routers or one end is not configured with EIGRP, no EIGRP routes will appear in the routing table of either router, because they will not have formed an EIGRP neighbor relationship. In this situation you will be able ping between the routers, but you will not be able to ping LANs attached to the other router.

The router eigrp command is incorrect because you need to specify the autonomous system number after the command to enable EIGRP in a network. The router eigrp 10 command includes the autonomous-system parameter.

The network 192.168.1.1 and network 10.2.2.2 commands are incorrect because the command must be in terms of the network or subnet ID of the network in which the interfaces reside. It is not entered in terms of the address of the interfaces.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > Cisco IOS Software > Configuring EIGRP > Enabling EIGRP

QUESTION 208
Which Cisco IOS command will display the following partial output?

```
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-demand routing, 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

Gateway of last resort is 10.30.10.85 to network 10.71.0.0

E 168.28.0.0 [140/8] via 10.212.215.122, 0:03:34, serial0/0
E 172.43.0.0 [140/8] via 10.145.231.221, 0:43:54, Ethernet 2
```

A. show ip
B. show ip route
C. show ip route summary
D. show route summary

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show ip route command will display the output in this scenario. The command is used to display the present status of the routing table. The complete command syntax is:

show ip route [[ip-address [mask] [longer-prefixes]] | [protocol [process-id]] | [list access-list-number | access-list-name]]

The following is a sample partial output:

```
D 168.28.0.0 [140/8] via 10.212.215.122, 0:03:34, serial0/0
```

The first letter represents the routing protocol through which the route is learned. In this case, the route is learned by EIGRP. The command output also lists codes used for all the routing protocols.

The routing protocol code is followed by the IP address of the remote network.

The first number in the bracket represents the administrative distance of the routing protocol. The number followed by slash within the bracket represents the cost of the route. Different routing protocol uses different methods to calculate the cost of the route. The IP address followed by the keyword via shows the next router

to the remote network. The next set of numbers is the time when the route was last updated, which is 0:03:34 in the example. Lastly, it displays the interface through which the network can be reached, which is serial0/0 in the example.

The show ip command is incorrect because it is not a valid Cisco IOS command.

The show ip route summary command is incorrect because this command is used to view the current state of the routing table.

The show route summary command is incorrect because it is not a valid Cisco IOS command.

Objective:
Routing Fundamentals Sub-
Objective:
Interpret the components of routing table

References:

QUESTION 209
As part of a new initiative to tighten the security of your Cisco devices, you have configured the firewall to restrict access to the devices from the outside.

What would be other recommended ways of protecting the integrity of the device configuration files on the devices while ensuring your continued ability to manage the devices remotely? (Choose all that apply.)

A. encrypt the configuration files
B. use SSH to connect to the devices for management
C. prevent the loss of administrator passwords by disabling their encryption
D. disable the VTY ports on the devices
E. use an encrypted password for VTY access

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should use SSH to connect to the devices for management. You should also require an encrypted password for VTY access. Using Telnet for remote management transmits all information, including the username and passwords, in clear text. Using an encrypted password for VTY access ensures that the password cannot be read either in transit or in the configuration file.

Passwords used for access to the console, aux, or VTY connections can be encrypted if desired. When passwords are created with the enable <password> command, the password is saved in clear text. When the enable secret <password> command is used, however the password will be encrypted.

If both types of password are configured for a particular connection type, the system will ignore the enable password and require the enable secret password. For example, if the set of commands shown below were executed, both types of password will be created for console access, but the system will require the password crisco rather than cisco. Also make note that neither of those passwords will required for VTY access. That password is sicso, which is the password configured after accessing the line VTY interface configuration prompt.

Router(config)# enable secret crisco
Router(config)# enable password cisco
Router(config)# line vty 0
4
Router(config-line)# password sisco

Although it is possible to encrypt the password in the configuration files, it is not possible to encrypt the rest of the files.

You should not disable the encryption of the passwords in the configuration files. Password encryption is a good security measure to take, and sloppy password management should not be a reason to change this practice.

You should not disable the VTY ports on the devices. This would certainly enhance security, but it would prevent you from managing the devices remotely

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco IOS Security Configuration Guide, Release 12.2>Security Overview

QUESTION 210
You have implemented the following IP SLA configuration, as shown in the following partial output of the show run command:

```
ip sla 1 dns cow.cisco.com name-server
10.52.128.30 ip sla schedule 1 start-time
now
```

Which of the following statements is true of this configuration?

A. It will find the response time to resolve the DNS name cow.cisco.com
B. It will find the response time to connect to the DNS server at 10.52.128.30
C. It will start in one minute
D. It will gather data from one minute

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:
It will find the response time to resolve the DNS name cow.cisco.com. Domain Name System (DNS) response time is computed by calculating the difference between the time taken to send a DNS request and the time a reply is received. The Cisco IOS IP SLAs DNS operation queries for an IP address if the user specifies a hostname, or queries for a hostname if the user specifies an IP address.

It will not find the response time to connect to the DNS server at 10.52.128.30. That is the IP address of the DNS server being used for the operation (10.52.128.30). However, it will measure the response time to resolve the DNS name cow.cisco.com.

It will not start in one minute. It will start immediately, as indicated by the start-time now parameter.

It will not gather data for one minute. The numeral 1 in the first line refers to the IP SLA number, and the numeral 1 in the last line refers to the IP SLA number to be scheduled.

Objective:
Infrastructure Management Sub-
Objective:
Troubleshoot network connectivity issues using ICMP echo-based IP SLA

References:
Home > Support > Technology support > IP > IP application services > Technology information > Technology white paper > Cisco IOS IP Service Level Agreements User Guide

QUESTION 211
Router 5 has four interfaces. The networks hosted on each interface are as follows:

```
Fa0/1     192.168.5.4/29
Fa0/2     192.168.6.0/24
Fa0/3     192.168.7.0/24
S0/0       172.16.5.0/24
```

You execute the following commands on the router:

```
Router5(config)# router bgp 20
Router5(config-router)# network 192.168.5.0
Router5(config-router)# network 192.168.6.0
Router5(config-router)# network 192.168.7.0
```

```
Router5(config-router)# network 172.16.5.0
Router5(config-router)# neighbor 172.16.5.2 remote-as 50
Router5(config-router)# aggregate-address 192.168.5.0 255.255.252.0
```

After this command sequence is executed, what routes will be present in the routing table of the router at 172.16.5.2? (Choose all that apply.)

A. 192.168.5.4/29
B. 172.16.5.0/24
C. 192.168.6.0/24
D. 192.168.7.0/24
E. none of these will be present
F. only network addresses beginning with 192 will be present

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Despite the inclusion of the command aggregate-address 192.168.5.0 255.255.252.0, all subnets of the aggregate route will also be placed in the routing updates because of the omission of the summary-only keyword. Therefore, 192.168.5.4/29, 172.16.5.0/16, 192.168.6.0/24 and 192.168.7.0/24 will be present.

Had the following command been executed, the subnet addresses would not appear in the routing table of the router at 172.16.5.2:

Router5(config-router)# aggregate-address 192.168.5.0 255.255.252.0 summary-only

Therefore, both the aggregate address and all of the 192.168.0.0 subnets will be in the routing table.

The 172.16.5.0/24 network will be in the routing table of the router at 172.160.5.1 because it is directly connected.

Objective: WAN
Technologies Sub-
Objective:
Configure and verify single-homed branch connectivity using eBGP IPv4 (limited to peering and route advertisement using Network command only)

References:
Cisco > Cisco IOS IP Routing: BGP Command Reference > aggregate-address

QUESTION 212

Which of the following are characteristics of Open Shortest Path First (OSPF)? (Choose three.)

A. Administrative distance of OSPF is 90
B. Administrative distance of OSPF is 110
C. OSPF uses the Dijkstra algorithm to calculate the SPF tree
D. OSPF uses the Diffusing Update algorithm (DUAL) algorithm to calculate the SPF tree

E. OSPF uses 224.0.0.5 as multicast address for ALLDRouters
F. OSPF uses 224.0.0.6 as multicast address for ALLDRouters

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following are characteristics of Open Shortest Path First (OSPF) routing protocol:
- The default administrative distance is 110.
- It uses 224.0.0.6 as the multicast address for ALLDRouters.
- It uses the Dijkstra algorithm to calculate the Shortest Path First (SPF) tree.

It uses Internet Protocol (IP) protocol 89.
- OSPF supports Non-Broadcast Multi-Access (NBMA) networks such as Frame Relay, X.25, and Asynchronous Transfer Mode (ATM). The default hello interval for NBMA networks is 30 seconds.
- OSPF supports point-to-point and point-to-multipoint connections.
- It also supports authentication.
- OSPF uses 224.0.0.5 as the multicast address for ALLSPFRouters.
- It uses link-state updates and SPF calculations that provides fast convergence.
- OSPF is recommended for large networks due to good scalability.

It uses cost as the default metric.
- There is no maximum hop count as with distance vector routing protocols. The number of hops to a network can be unlimited.

The option stating that AD of OSPF is 90 is incorrect because 90 is the default administrative distance for an internal Enhanced Interior Gateway Routing Protocol (EIGRP) route.

The option stating that OSPF uses the Diffusing Update algorithm (DUAL) algorithm to calculate the SPF tree is incorrect. The DUAL algorithm is used by EIGRP to calculate the SPF tree.

Keep the following in mind when comparing OSPF and EIGRP:
- EIGRP is vendor specific; OSPF is not

- EIGRP has an AD of 90; OSPF has an AD of 110
- OSPF elects a DR on each multi-access network; EIGRP does not
- OSPF uses cost as its metric, and EIGRP uses bandwidth as its metric

The option stating that OSPF uses 224.0.0.5 as multicast address for ALLDRouters is incorrect because OSPF uses 224.0.0.6 as multicast address for ALLDRouters, and 224.0.0.5 as multicast address for ALLSPFRouters.

Objective:
Routing Fundamentals Sub-
Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:
Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039
Cisco > Support > IP > IP Multicast > Technology Information > Technology Briefs > Internet Protocol IP Multicast Technology

QUESTION 213
Which Cisco Internetwork Operating System (IOS) command is used to encrypt passwords on Cisco routers?

A. password secure
B. service encryption-password
C. service password-encryption
D. enable password

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The service password-encryption command is used to encrypt passwords on Cisco routers. It is used to encrypt all passwords configured on the router, both current and future. This means all passwords in the plain text configuration file will be encrypted. This command is issued in global configuration mode. The syntax of the command is as follows:

Router(config)# service password-encryption

This command does not have any parameters.

Once executed any password in the configuration file will appear similar to what is shown below when the running or startup configuration files are viewed:

```
R1#show run <output
omitted> line console 0
password 7 09-4f60C0B1C1B
login
<output omitted>
```

The password secure and service encryption-password commands are incorrect because they are not valid Cisco IOS commands.

The enable password command is used to set the privileged EXEC mode password, and does not encrypt the password by default.

Objective:
Infrastructure Security Sub-
Objective:
Configure, verify, and troubleshoot basic device hardening

References:
Cisco > Cisco IOS Security Configuration Guide, Release 12.4 > Part 7: Secure Infrastructure > Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

QUESTION 214
Which statement correctly identifies a difference between Inter-Switch Link (ISL) and 802.1q?

A. 802.1q uses a native VLAN, ISL does not.
B. Cisco devices support only ISL.
C. ISL uses a 12-bit VLAN number field, and 802.1q does not.
D. ISL modifies the original Ethernet frame, while 802.1q encapsulates the original Ethernet frame.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
802.1q defines a native virtual LAN (VLAN) on each trunk link, which defaults to VLAN 1. The 802.1q frame tagging method specifies that frames in the native VLAN will not be tagged while transmitting over a trunk link. The switch on the other end of the link identifies a native VLAN frame by the absence of the 802.1q header. ISL does not have the concept of native VLANs, and traffic from all VLANs is encapsulated.

While older Cisco devices support both the ISL and 802.1q frame tagging methods, ISL is a deprecated, Cisco-proprietary frame tagging method, and newer Cisco switches only support the 802.1q standard. When switches from multiple vendors are installed in the network, the 802.1q frame tagging method should be used.

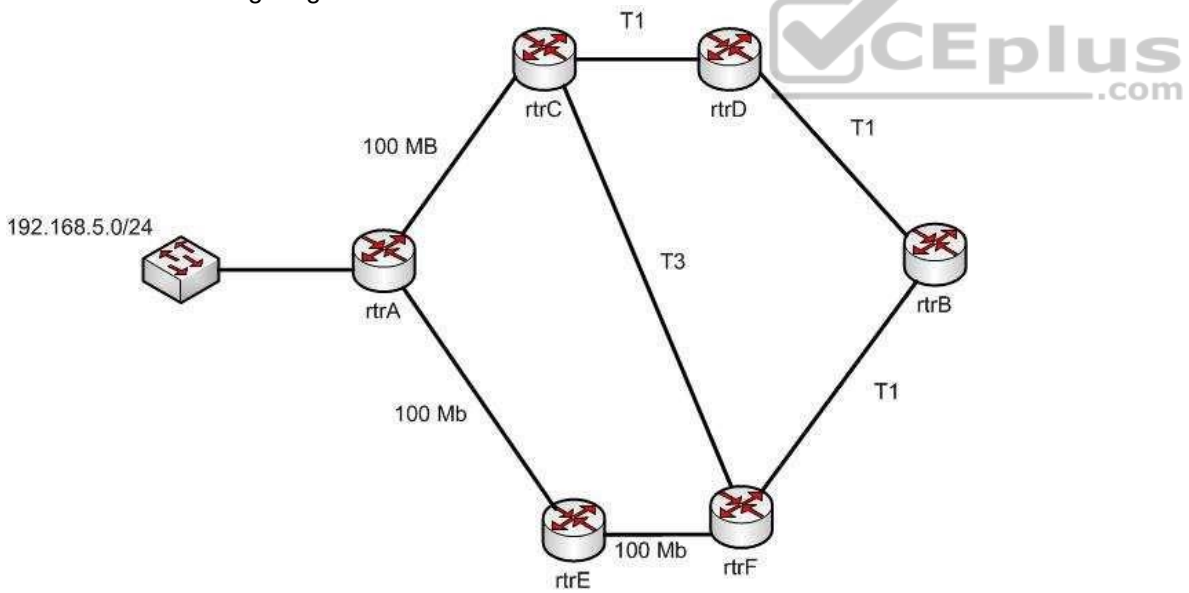
It is incorrect to state that ISL uses a 12-bit VLAN number field and 802.1q does not. ISL uses a 15-bit VLAN ID field, while 802.1q uses a 12-bit VLAN ID field.

ISL encapsulates the original Ethernet frame, adding a 26-byte header and a 4-byte trailer. 802.1q operates by inserting a 4-byte header inside the original Ethernet frame, then recalculating the checksum (CRC) in the Ethernet trailer.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format > Document ID: 17056

QUESTION 215
Examine the following diagram:



While troubleshooting an OSPF routing problem, you need to determine the cost for Router F to reach the 192.168.5.0 24 network via the best route.

What will that cost be?

A. 110
B. 2
C. 3
D. 7

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
The best route to the 192.168.5.0/24 network from the perspective of router F will have an OSPF assigned cost of 2. There are three possible loop-free paths to get from router F to the 192.168.5.0/24 network. The default OSPF costs for a 100 MB link, a T1 link, and a T3 link are 1, 64, and 2, respectively.

The three paths and the calculation of their costs are shown:

Router F to Router E to Router A: 1 + 1 = 2
Router F to Router C to Router A: 2 + 1 = 3
Router F to Router B to Router D to Router C to Router A: 64 + 64 + 64 + 1 = 193

Each OSPF route calculates the cost of its path to a network, and passes that value on to the next router, which will then add to it the cost to reach that neighbor. For example, the routing table of Router E would look like this for the route to 192.168.5.0/24:

```
O 192.168.5.0 [110/1] via <output omitted>
```

Router F would add its own cost to reach Router E to the cost of reaching 192.168.5.0/24, resulting in the following output:

```
O 192.168.5.0 [110/2] via <output omitted>
```

110 is the administrative distance of OSPF.

Objective:
Routing Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

QUESTION 216
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:

Cisco > Cisco IOS IPv6 Configuration Guide, Release 12.4 > Implementing IPv6 Addressing and Basic Connectivity > IPv6 Address Formats
Cisco > Internetworking Technology Handbook > IPv6

QUESTION 217
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 new switch 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/extended range) spanning multiple switches

References:
Cisco > Support > LAN Switching > Virtual LANS / VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Configuring VLAN Trunk Protocol (VTP) > Document ID: 98154
Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25) > Understanding and Configuring VLANs, VTP, and VMPS

QUESTION 218
You have a Telnet session established with a switch from a router. You would like to maintain that connection while you return to the session with the router, and then easily return to the switch session after connecting to the router.

What command should you use?

A. <Ctrl-Shift-6>x
B. resume
C. suspend
D. <Ctrl-Alt-6>shift

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
After typing the Ctrl-Shift-6 sequence, you can tap the x key and return to the previous session, which in this case was the session with the router. Below is the full sequence of commands described in this item:

```
Router1#telnet 192.168.3.3
```

```
Tying 192.168.3.3..Open
User Access Verification
Password:
Switch2><Ctrl-Shift-6>x
Router1#
```

When you desired to return to the session with the switch, you would use the resume command as shown below:

```
Router1#resume
Switch>
```

Neither the suspend nor the <Ctrl-Alt-6>shift commands are valid commands.

Objective:
Infrastructure Management Sub-
Objective:
Perform device maintenance

References:
Establishing Telnet Sessions>Suspending and Terminating Telnet Sessions

QUESTION 219
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 Management Sub-
Objective:
Configure and verify initial device configuration

References:
Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 6: Using the Cisco IOS Integrated File System > NVRAM File System Management
Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 11: Rebooting > Rebooting and Reloading - Configuring Image Loading Characteristics

QUESTION 220
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 serial 0. This subcommand is not functional while you are still in privileged mode.

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

References:
Cisco > Cisco 1600 Series Software Configuration Guide > Cisco IOS Software Basic Skills

QUESTION 221
Which Cisco IOS command will enable a switch to copy the configuration from NVRAM to its RAM?

A. copy tftp flash
B. copy running-config flash
C. copy startup-config flash
D. copy startup-config running-config
E. copy running-config startup config

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The copy startup-config running-config command enables a switch (or a router) to copy configuration from NVRAM to its RAM. The configuration file located in NVRAM is referred to as the startup configuration, and a configuration currently loaded and running in RAM is referred to as the running configuration.

The copy running-config startup-config command is incorrect because it will save your running configuration in RAM to the non-volatile NVRAM, which is the reverse of the scenario's requirement. This would be the required command to run if you have edited the running configuration and would like to save the changes so that they are effective the next time you restart the switch.

The copy tftp flash command does not enable a switch to copy the configuration from NVRAM to its RAM. This command is used to restore backup IOS images stored on a TFTP server to the target switch (or router).

The copy running-config flash command does not enable a switch to copy the configuration from NVRAM to its RAM. This command is used to save the running configuration in RAM to the switch's flash memory.

The copy startup-config flash command does not enable a switch to copy the configuration from NVRAM to its RAM. This command is used to save the startup configuration in NVRAM to the switch's flash memory.

Objective:
Infrastructure Management Sub-
Objective:
Perform device maintenance

References:
Cisco > Cisco IOS Configuration Fundamentals Command Reference > C > copy
Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 8: Managing Configuration Files > Managing Configuration Files

QUESTION 222
A switch is powered up, and the system LED is amber.

Which of the following describes this situation?

A. The switch is malfunctioning.
B. Utilization level is high.
C. The switch is performing normally.
D. There is a security violation on a switch port.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The system LED indicates the overall health of the switch. The LED should turn solid green after a successful Power On Self Test (POST). An amber system LED indicates that there is a system-wide failure in the switch.

High utilization will not cause the system LED to turn amber.

An amber system LED indicates a general switch malfunction. It does not indicate that the switch is performing normally.

Port security violations will not cause the system LED to be amber. The system LED is used to identify the overall health of the switch.

Objective:
LAN Switching Fundamentals Sub-
Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:
Cisco > Catalyst 2960 Switch Hardware Installation Guide > LEDs

QUESTION 223
Which statement is true regarding Inter-Switch Link (ISL) frame tagging?

A. ISL uses a native VLAN.
B. ISL works with non-Cisco switches.
C. ISL adds a 26-byte trailer and 4-byte header.
D. The original Ethernet frame is not modified.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
With ISL frame tagging, the original Ethernet frame is not modified. ISL encapsulates the original frame by adding a 26-byte header and a 4-byte Cyclic Redundancy Check (CRC) trailer. The original Ethernet frame is placed between the header and trailer. A normal Ethernet frame can have a maximum size of 1,518 bytes, and therefore adding the header and trailer size gives an ISL frame a maximum size of 1,548 bytes.

ISL frame tagging does not use the concept of a native VLAN. Instead, Institute of Electrical and Electronics Engineers (IEEE) 802.1q frame tagging uses the native VLAN. Unlike ISL trunks, where every frame traversing the trunk is tagged with an ISL header and a trailer, 802.1Q trunks allow untagged frames over the native VLAN. An untagged frame does not carry VLAN identification information in it and is a simple Ethernet frame.

ISL is proprietary to Cisco, and thus does not work with non-Cisco switches.

ISL frame tagging does not add a 26-byte trailer and 4-byte header. It adds a 26-byte header and 4-byte trailer.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure and verify Layer 2 protocols

References:
Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format > Document ID: 17056

QUESTION 224
You have two routers in your OSPF area 0. Router 1 is connected to Router 2 via its Serial 1 interface, and to your ISP via the Serial 0 interface. Router 1 is an ASBR.

After your assistant configures a default route on Router 1, you discover that whenever either router receives packets destined for networks that are not in the routing tables, it causes traffic loops between the two routers.

To troubleshoot, you execute the show run command on Router 1. Part of the output is shown below:

```
<output omitted>
IP route 0.0.0.0 0.0.0.0 serial 1
Router ospf 1
```

```
Network 192.168.5.0 0.0.0.255 area 0 Default-
information originate
```

Which command or set of commands should you execute on Router 1 to stop the looping traffic while maintaining Router 2's ability to send traffic to the Internet?

A. Execute the no default-information originate command.
B. Execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command and then execute the ip route 0.0.0.0 0.0.0.0 serial 0 command.
C. Execute the default-information originate always command.
D. Execute the no network 192.168.5.0 area 0 command and then execute the network 192.168.5.0 255.255.255.0 area 0 command.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command followed by the ip route 0.0.0.0 0.0.0.0 serial 0 command. The original configuration command was executed on the wrong interface on Router 1 by your assistant. It should be executed on Serial 0, which is the connection to the ISP. The show run command indicates that with the current configuration, if Router 2 receives a packet not in its table, it sends it to Router 1, and then Router 1 sends it back out on Serial 1. This redirects the packet back to Router 2, and the loop begins. By changing the configuration to Serial 0, Router 1 will start forwarding all traffic not in the routing table to the ISP.

You should not execute the no default-information originate command. This command instructs Router 1 to NOT inject the default route into area 0, which is the desired behavior. Running this command would stop the loop, but would leave Router2 with no default route to send packets to the Internet.

You should not execute the default-information originate always command. The addition of the always parameter instructs Router 1 to inject a default route into area 0, even if one does not exist on Router 1. This is unnecessary, since Router 1 does have a default route configured, and will not change the existing looping behavior.

You should not execute the no network 192.168.5.0 area 0 command followed by the network 192.168.5.0 255.255.255.0 area 0 command. There is nothing wrong with the original network command. Also, the network 192.168.5.0 255.255.255.0 area 0 command uses an incorrect mask type. The mask must be in the wildcard format. Moreover, since it is incorrect, this will have the effect of disabling OSPF on the network connecting the two routers.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

QUESTION 225
Which subnet is IP address 172.16.5.2 /23 a member of, and what is the broadcast address for that subnet?

A. subnet: 172.16.4.0, broadcast: 172.16.5.255
B. subnet: 172.16.5.0, broadcast: 172.16.5.255
C. subnet: 172.16.2.0, broadcast: 172.16.5.255
D. subnet: 172.16.0.0, broadcast: 172.16.7.255

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IP address 172.16.5.2 /23 is a member of subnet 172.16.4.0 and has the broadcast address of 172.16.5.255. The valid host range is between 172.16.4.1 and 172.16.5.254.

Binary form of IP address 172.16.5.2 = 10101100.00010000.00000101.00000010
Binary conversion for /23 netmask = 11111111.11111111.11111110.00000000
Decimal conversion for /23 netmask = 255.255.254.0

Calculations:

Perform the AND operation between the IP address and the netmask to obtain the subnet ID:

Address = 10101100.00010000.00000101.00000010
Netmask = 11111111.11111111.11111110.00000000

Subnetwork ID = 10101100.00010000.00000100.00000000

Convert the binary version of the network ID to dotted decimal format, 172.16.4.0.

To obtain the broadcast address, replace the last 9 host bits (32 - 23 = 9 bits) of the network address, which yields the following:

Binary form of broadcast address = 10101100.00011001.00000101.11111111
Decimal form of broadcast address = 172.16.5.255

Subnet	0.0	2.0	4.0
First Host	0.1	2.1	4.1
Last Host	1.254	3.254	5.254
Broadcast Address	1.255	3.255	5.255

Objective:
Network Fundamentals Sub-
Objective:
Apply troubleshooting methodologies to resolve problems

References:
Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses
Cisco > Technology Support > IP > IP Addressing Services > Design TechNotes > Subnet Zero and the All-Ones Subnet > Document ID: 13711

QUESTION 226
You just finished configuring VLAN Trunking Protocol (VTP) in a network containing five switches. One of the switches is not receiving VLAN information from the switch that is acting as the server.

Which of the following could NOT be a reason why the switch is not receiving the information?

A. The VTP domain name on the switch may be misspelled
B. The VTP password may be misspelled on the switch
C. The configuration revision number may be out of sync
D. The VTP version used on the switch may be different

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The configuration revision number does not need to match on the switches. The configuration number cannot be directly configured, but is instead synchronized during VTP updates.

For VTP to function correctly, all of the following conditions must be true:
- The VTP version must be the same on all switches in a VTP domain.
- The VTP password must be the same on all switches in a VTP domain.

- The VTP domain name must be the same on all switches in a VTP domain.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot STP protocols

QUESTION 227
You need to configure Network Address Translation (NAT) to allow users access to the Internet. There are 62 private hosts that need Internet access using the private network 10.4.3.64 /26, and all of them will be translated into the public IP address of the serial interface.

Which of the following NAT configurations will allow all 62 hosts to have simultaneous Internet access?

A. Router(config)# ip nat pool POOLNAME 10.4.3.64 /26
Router(config)# interface s0
Router(config-if)# ip nat inside source 1 pool POOLNAME overload
B. Router(config)# access-list 1 permit 10.4.3.64 0.0.0.127
Router(config)# interface s0/0
Router(config-if)# ip nat source list 1 pool POOLNAME overload
C. Router(config)# access-list 1 permit 10.4.3.64 /26
Router(config)# ip nat inside source list 1 interface serial 0
D. Router(config)# access-list 1 permit 10.4.3.64 0.0.0.63
Router(config)# ip nat inside source list 1 interface serial 0 overload

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should execute the following commands:

Router(config)# access-list 1 permit 10.4.3.64 0.0.0.63
Router(config)# ip nat inside source list 1 interface serial 0 overload

A successful NAT configuration requires the creation of an access control list (ACL) to identify the private IP addresses that will be translated, as well as an ip nat inside source command to dictate what public IP addresses will be used for translation. Cisco uses the term "inside local" for IP addresses prior to translation, and "inside global" for public IP addresses after translation.

The access-list 1 permit 10.4.3.64 0.0.0.63 command correctly identifies the private host network of 10.4.3.64 /26, consisting of 62 hosts.

The ip nat command is broken down as follows:
▪ inside: indicates that packets received on the inside (private) interface will be translated
▪ list 1: specifies that access list 1 will be used to determine which private IP addresses will be translated ▪ interface serial 0: specifies that NAT will translate private IP addresses into the IP address of the serial 0 interface ▪ overload: allows NAT to reuse the IP address of the serial interface for all private IP addresses, providing them simultaneous access to the Internet

The correct wildcard mask is critical to ensuring that the access list allows translation of all LAN devices. For example, if the private LAN used the 192.168.9.0/24 network and 167 devices were present in the network, the correct wildcard mask would be 0.0.0.255. If you used an incorrect wildcard mask, such as 0.0.0.3, only the 192.168.9.0/30 network would be allowed translation (only the IP addresses 192.18.9.1 and 192.168.19.2.) Of the 167 devices, 165 would not receive translation.

The overload keyword is required in this configuration, since there are more private IP addresses (62) than there are public IP addresses (one). Overload activates NAT overloading, often called Port Address Translation (PAT), and assigns each private IP address a unique, dynamic source port in router memory to track connections. If the overload keyword were not included in the NAT configuration, only one private host could access the Internet at a time.

An alternate solution would involve the creation of a pool of public IP addresses on the NAT router, and applying the access control list to the NAT pool:

Router(config)# ip nat pool NATPOOL 201.52.4.17 201.52.4.22 netmask 255.255.255.248
Router(config)# ip nat inside source list 1 pool NATPOOL overload

The first command creates a NAT pool with six public IP addresses on subnet 201.52.4.16/29, which will be used for translation. The second command then ties access list 1 to the NAT pool, and specifies overload so that the six public addresses can be reused as often as necessary, allowing all of the private IP addresses simultaneous Internet access.

In both of these examples, dynamic mapping is used. Without dynamic mapping, it is not possible for computers from outside the network to establish a connection with computers inside the network unless a static mapping between the private IP address and the public IP address is established on the NAT device.

A common alternative approach is to use public IP addresses in the DMZ rather than private IP addresses, and to place any computers than must be accessed from outside the network in the DMZ. In this case, NAT is not required between the DMZ devices and the Internet. Even if public IP addresses are used in the DMZ, if the addresses undergo NAT translation, connections from outside the network will not be possible.

When NAT is used to translate a public IP address (or addresses) to private IP addresses, the NAT process is ONLY implemented on the router that connects the network to the Internet. This is because private IP addresses are not routable to the Internet, and translation must occur where the network connects to the Internet.

The following command sets are incorrect because they both involve the creation of a NAT pool:

Router(config)# ip nat pool POOLNAME 10.4.3.64 /26
Router(config)# interface s0
Router(config-if)# ip nat inside source 1 pool POOLNAME overload

and

Router(config)# access-list 1 permit 10.4.3.64 0.0.0.127
Router(config)# interface s0/0
Router(config-if)# ip nat source list 1 pool POOLNAME overload

The scenario states you must use the IP address of the serial interface as the public address. Also, the ip nat inside source command is configured in global configuration mode, not interface configuration mode. Finally, access control lists require inverse masks (such as 0.0.0.63). CIDR notation (as in POOLNAME 10.4.3.64 /26) is not allowed.

The following command set is incorrect because access control lists require inverse masks (such as 0.0.0.63) and CIDR notation (/26) is not allowed:

Router(config)# access-list 1 permit 10.4.3.64 /26
Router(config)# ip nat inside source list 1 interface serial 0

Also, the ip nat inside source command is configured in global configuration mode, not interface configuration mode.

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

References:

QUESTION 228
At which of the following layers of the Cisco three-tier architecture should port security be implemented?

A. Access layer
B. Distribution layer
C. Core layer
D. Edge layer

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Port security is one of the functions that should be performed at the Access layer. Among other functions that are done at this layer are:
- PoE
- Link aggregation
- QoS

Port security should not be performed at the Distribution layer. Among the functions that should be done at this layer are: ▪
Routing updates
- Route summaries
- VLAN traffic
- Address aggregation

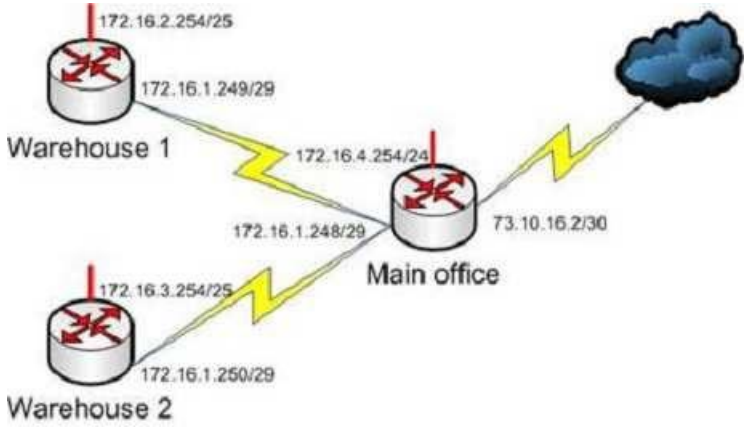
Port security should not be performed at the Core layer. Among the functions that should be done at this layer are: ▪
Access-list checking
- Data encryption
- Address translation

Edge is not one of the three layers in the Cisco three-tier model.

Objective:
Network Fundamentals Sub-
Objective:
Compare and contrast collapsed core and three-tier architectures

References:
Cisco Press > Articles > Cisco Network Technology > General Networking > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design
Study CCNA > Cisco three-layer hierarchical model

QUESTION 229
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

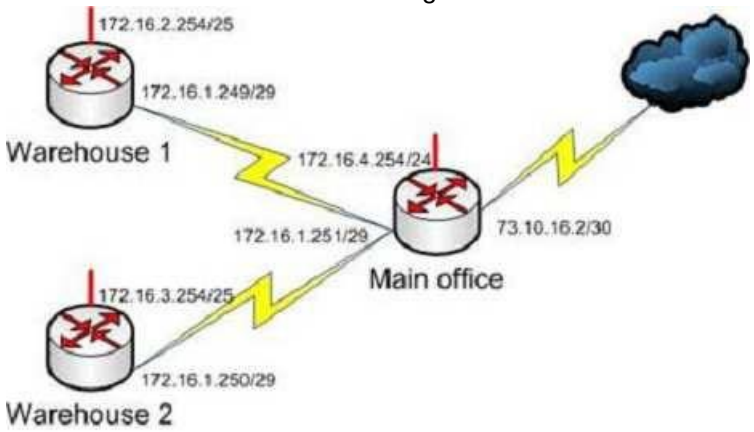
172.16.0.40

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:
IP Addressing and Subnetting for New Users

QUESTION 230

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 Software IOS (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.
2 Ethernet/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 of 2102 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 2142 is 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 Management Sub-
Objective:
Use Cisco IOS tools to troubleshoot and resolve problems

References:
Cisco > Product Support > Routers > Cisco 10000 Series Routers > Troubleshoot and Alerts > Troubleshooting TechNotes > Use of the Configuration Register on All Cisco Routers > Document ID: 50421
Cisco > Cisco IOS Configuration Fundamentals Command Reference > config-register

QUESTION 231
Which of the following is NOT a packet type used by Enhanced Interior Gateway Routing Protocol (EIGRP)?

A. Query
B. Reply

C. Ack
D. Response

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Response is not a packet type used by EIGRP. The following are the packet types used by EIGRP:
▪ Hello/Ack: Establish neighbor relationships. The Ack packet is used to provide acknowledgement of a reliable packet. ▪
Update: Send routing updates.
▪ Query: Ask neighbors about routing information.
▪ Reply: Provide response to queries about routing information.
▪ Requests: Gain specific information from one or more neighbors.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > Cisco IOS Software > Configuring EIGRP

QUESTION 232
Which of the following technologies allows a switch port to immediately transition to a forwarding state?

A. Rapid STP
B. PortFast
C. VTP
D. CDP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

PortFast is a technology that allows a switch port connected to an end node such as a workstation, server, or printer to bypass the normal Spanning Tree Protocol (STP) convergence process. When a new device is powered up on a switch port, it will immediately transition to a forwarding state.

NOTE: PortFast should only be used on access ports. It should not be used on trunk ports or on ports that connect to hubs, routers and other switches.

Rapid STP (RSTP) is a new STP standard that provides faster convergence than the original 802.1d STP. RSTP supports PortFast, but it must be configured explicitly.

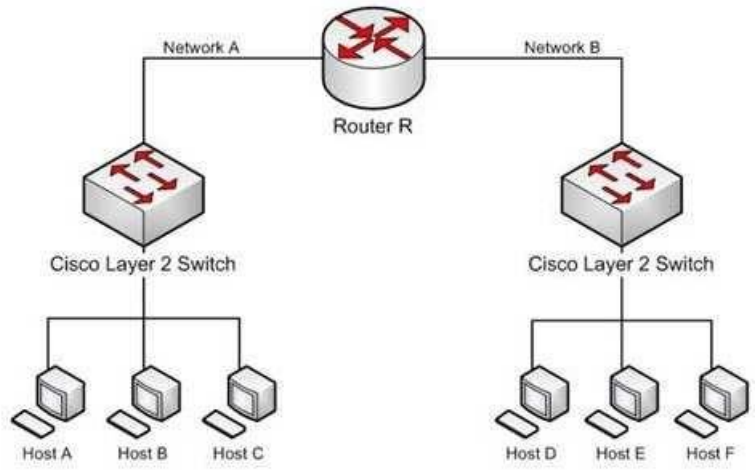
The VLAN Trunking Protocol (VTP) does not allow for immediate transition to a forwarding state. VTP is used to synchronize VLAN databases between switches, and has no effect on STP.

The Cisco Discovery Protocol (CDP) does not allow for immediate transition to a forwarding state. CDP is used to verify connectivity and document directly connected Cisco devices. CDP is not related to STP.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP-related optional features

References:
Cisco > Support > Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, and LoopGuard > Understanding How PortFast Works

QUESTION 233
Refer to the network diagram in the exhibit. Host A is configured with an incorrect default gateway. All other computers and the Router are known to be configured correctly (Click the Exhibit(s) button.)



Which of the following statements is TRUE?

A. Host C on Network A cannot communicate with Host A on Network A.
B. Host A on Network A can communicate with all other hosts on Network A.
C. Host A on Network A can communicate with Router R.

D. Host C on Network A cannot communicate with Router R.
E. Host D on Network B cannot communicate with Host B on Network A.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Host A on Network A can communicate with all other hosts on Network A and with Router R. To communicate with local hosts and the interface of Router R (which are all in the same subnet) only a correct IP address is reqired. If the default gateway of Host A is incorrect, then it will not be able to communicate with any host on the other side of the router, which includes Network B in the diagram. Packets from hosts on Network B will reach Host A on Network A without any problem, because they possess the correct address of the default gateway or router, but Host A will send the packet to a dead end because Host A has an incorrect default gateway. On the other hand, Host A does not require a default gateway to communicate with other hosts on same network.

Host C on Network A WILL be able to communicate with Host A on Network A , even though Host A has an incorrect default gateway because Host A and C are in the same subnet, which requires no use of the of the gateway or router..

Host C on Network A WILL be able to communicate with Router R because Host C has the correct default gateway address which is the address of Router R.

Host D on Network B WILL be able to communicate with Host B on Network A because both hosts have a correct default gateway address.

Objective:
Routing Fundamentals Sub-
Objective:
Troubleshoot basic Layer 3 end-to-end connectivity issues

References:
Cisco > Internetworking Technology Handbook > Internetworking Basics > Routing Basics
http://www.microsoft.com/technet/community/columns/cableguy/cg0903.mspx
http://kb.iu.edu/data/ajfx.html

QUESTION 234
When transmitting to a remote destination, what two things will occur after a host has determined the IP address of the destination to which it is transmitting? (Choose two.)

A. The sending host will perform an ARP broadcast in its local subnet using the IP address of the destination host.
B. The sending host will perform an ARP broadcast in its local subnet using the IP address of the local router interface.
C. The local router interface will respond with the MAC address of the destination host.
D. The local router interface will respond with its own MAC address.
E. The destination host will respond with its own MAC address.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When a transmission is made to a remote location, the sending host will perform an Address Resolution Protocol (ARP) broadcast in its local subnet using the IP address of the local router interface, and the local router interface will respond with its own MAC address. A remote address is defined as an address in a different subnet.

When a host determines (through a process called ANDing) that a destination address is remote, it will send the packet to the local router interface, which is known as the default gateway on the host. But when it performs ANDing on the IP address of the local router interface, it will discover that the interface is local. When

transmitting to a local IP address, a conversion to a MAC address must occur. Therefore, it will perform a local ARP broadcast, and the local router interface will respond with its MAC address.

Regardless of whether the host is broadcasting for the MAC address of the destination locally on the same LAN, or if it is broadcasting for the MAC address of the router interface (remotely), the broadcast will be a Layer 2 broadcast using the MAC address ff-ff-ff-ff-ff-ff. It will be received by all devices on the LAN, but only the device with the specified IP address will reply.

The ARP resolution process does take a second or two to complete if no mapping for the destination devices IP address to MAC address is found in the ARP cache. For example, if the MAC address must be resolved through the ARP broadcast when pinging from one device to another, it can cause the first several echo requests to go unanswered, as shown on the output below. After this resolution has been completed, however, the second ping attempt should receive an answer to all five ICMP echo requests.

```
Router1#ping 50.6.3.26

Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 50.6.3.26, timeout is 2 seconds:
..!!!

Router1#ping 50.6.3.26

Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 50.6.3.26, timeout is 2 seconds:
!!!!!
```


The sending host will not perform an ARP broadcast in its local subnet using the IP address of the destination host. A local ARP broadcast is only performed when the ANDing process deduces that the destination IP address is local. In this case, the destination is remote.

The destination host will not respond with its MAC address. The process of learning the MAC address of the destination computer is the responsibility of the local router interface on the subnet where the destination host resides.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Describe and verify switching concepts

References:
Cisco > Cisco IOS XR IP Addresses and Services Configuration Guide for the Cisco XR 12000 Series Router, Release 4.3.x > Configuring ARP

QUESTION 235
Which command enables HSRP on an interface?

A. hsrp
B. standby ip
C. standby mode hsrp
D. switchport mode hsrp

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The standby ip interface configuration command enables Hot Standby Router Protocol (HSRP). The syntax for this command is as follows:

switch(config-if)# standby group-number ip ip-address

The group-number argument specifies the HSRP group number on the interface. You do not need to enter a group number if there is only one HSRP group.

At least one interface on one of the routers in the group must be configured with the virtual IP address of the group. It is optional on all other interfaces on the other routers, which can learn the address through the hellos sent among the group.

A complete HSRP configuration is shown below with an explanation of each command.

```
RouterA (config) #interface Fa0/1
RouterA (config-if) # ip address 192.168.5.6 255.255.255.0
RouterA (config-if) # standby 2 ip 192.168.5.10
RourerA(config-if) # standby 2 priority 150
RouterA (config-if) #standby 2 Preempt
RouterA(config-if) #standby 2 track interface fa0/2
```

- Line 1 specifies the interface
- Line 2 addresses the interface

- Line 3 specifies the HSRP group number and the virtual IP address -
Line 4 sets the HSRP priority
- Line 5 allows the router to take the active role if its priority becomes higher than that of the active router

In the above, the router is tracking its own Fa0/2 interface. If that interface goes down it will reduce its priority by 10 (this is the default decrement when not specified). The new value would be 140 if that happened. To specify a decrement value, add it to the track command, as in this example: track interface Fa0/2 20.

When you configure routers to be part of an HSRP group, they listen for the HSRP MAC address for that group as well as their own burned-in MAC addresses.

HSRP uses the following MAC address:
0000.0c07.ac** (where ** is the HSRP group number)

The switchport mode interface configuration command will configure the VLAN membership mode of a port. It is not used to enable HSRP.

The options standby mode hsrp and hsrp are not valid commands.

Objective:
Infrastructure Services Sub-
Objective:
Configure, verify, and troubleshoot basic HSRP

References:
Cisco > Home > Technology Support > IP > IP Application Services > Design > Design Technotes > Hot Standby Router Protocol Features and Functionality
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 236
What IOS command produced the following output?

```
<output omitted>
Vlan Mac Address Type Ports
---- ------------ ------- -----
1 0040.63d8.ba0a DYNAMIC Fa0/1
1 0004.274c.9ca0 DYNAMIC Fa0/3
1 0040.63d8.bab8 DYNAMIC Fa0/10
1 000f.1fd3.d85a DYNAMIC Fa0/7
<output omitted>
```


A. show interface mac
B. show mac
C. show mac-address-table
D. show ip interface

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The output was produced by the show mac-address-table command. The show mac-address-table command displays a table of every learned MAC address and the switch port associated with the MAC address. The output shown in the question indicates that four MAC addresses have been learned by this switch, and the

last column indicates the switch port over which each MAC address was learned, and for which frames destined for each MAC address will be forwarded. The MAC address table is built dynamically by examining the source MAC address of received frames.

The show ip interface command is a router command, and displays no information on MAC address tables.

The show interface mac and show mac commands are incorrect because they are not valid Cisco IOS commands.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Describe and verify switching concepts

References:

QUESTION 237
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 through non-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 is 255.255.255.0
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:
Cisco > Cisco IOS IP Routing Protocols Command Reference > IP Routing Protocol-Independent Commands: S through T > show ip protocols

QUESTION 238
You apply the following commands to a router named R2:

```
R2(config)# interface Tunnel1
R2(config-if)# ip address 172.16.1.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 2.2.2.2
R2(config-if)# tunnel destination 1.1.1.1
```

Which statement is NOT true with regard to this configuration?

A. The physical IP address of R2 is 2.2.2.2
B. The connection will operate in IP mode
C. The configuration will increase packet fragmentation
D. The configuration alters the maximum segment size

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The configuration will not increase packet fragmentation. Conversely, it will reduce it by lowering the maximum transmission unit to 1400 and the maximum segment size to 1360 bytes.

Most transport MTUs are 1500 bytes. Simply reducing the MTU will account for the extra overhead added by GRE. Setting the MTU to a value of 1400 is a common practice, and it will ensure unnecessary packet fragmentation is kept to a minimum.

The other statements are true. The physical address of R2 is 2.2.2.2, while the tunnel interface address is 172.16.1.2.

Because you have not issued any command that changes the connection, it will operate in the default mode of IP.

The configuration does alter the maximum segment size with the ip tcp adjust-mss 1360 command.

Objective: WAN
Technologies Sub-
Objective:
Configure, verify, and troubleshoot GRE tunnel connectivity

References:
Home > Network Infrastructure > WAN, Routing and Switching > How to configure a GRE tunnel

QUESTION 239
Which Cisco IOS command configures the clock rate to 64,000 bits per second on an interface?

A. clock-rate 64000
B. clock rate 64k
C. clock rate 64000
D. clockrate 64000

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The clock rate 64000 command would configure the clock rate to 64,000 bits per second on an interface. The clock rate command is used to configure the clock rate for hardware connections on serial interfaces. These interfaces can be network interface modules (NIMs) and interface processors. The syntax of this command is clock rate bps.

A serial connection between two routers that are connected with a v.35 serial cable requires a clock rate on the Data Communications Equipment (DCE) end of the cable, but not on the Data Terminal Equipment (DTE) end. When the router is connected to a CSU/DSU for connection to the outside world, the DCE end will be the CSU/DSU. In a lab environment or any situation where you have two routers connected with this type of serial cable, a clock rate must be set on the DCE end of the cable.

When troubleshooting a connection of this type between routers, the state of the clock rate (set or unset) can be determined by running the show controllers command on the DCE end. The output will display as follows if the clock rate is NOT set:

```
Router#show controllers s0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 clocks stopped
```

```
More output omitted
```

Notice the DTE V.35 clocks stopped line, which indicates no clock rate is set. Another clue that there is a Layer 2 problem is the output of the show ip interface S0/0 command, executed on the same interface below:

```
Router# show ip interface s0/0
Serial0/0 is up, line protocol is down
Internet address is 192.168.1.2/24
Broadcast address is 255.255.255.255
```

Notice the Serial0/0 is up, line protocol is down line. Serial0/0 is up indicates that the physical connection is good, but line protocol is down indicates a problem with Layer 2 . If you were troubleshooting from the bottom layer to the top, you would now check Layer 2, which would be the clock rate.

If you want to change a DCE interface to a DTE device, you should use the no clock rate command.

All the other options are incorrect because these commands are syntactically incorrect.

Objective: WAN
Technologies Sub-
Objective:
Describe WAN access connectivity options

References:

QUESTION 240
Which of the following commands sets the local router to serve as an authoritative time source?

A. ntp server
B. ntp master
C. ntp authenticate
D. ntp peer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The ntp master command sets the local router to serve as an authoritative time source.

The ntp server command is used to specify an external time source that the local router should use as its time source.

The ntp authenticate command is used to enable the authentication of time source to which the local router has been configured to use. It is the first step in a process that must also include the specification of a hashing algorithm and a key, both of which must match on the time source.

The ntp peer command is used to configure the local router to synchronize a peer or to be synchronized by a peer. It does not make the local router authoritative as a time source like the ntp master command.

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

References:
Cisco > Support > Cisco IOS Basic System Management Command Reference > ntp master

QUESTION 241
File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP) work at which layer in the Open Systems Interconnection (OSI) model?

A. the Session layer
B. the Presentation layer
C. the Application layer
D. the Network layer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FTP and SMTP work at the application layer in the OSI model. The application layer is responsible for interacting directly with the application. It provides application services, such as e-mail and FTP. The following protocols work on the application layer:
- FTP: Used to transfer data between hosts through the Internet or a network.
- SMTP: A Transmission Control Protocol (TCP)/ Internet Protocol (IP) protocol used to send and receive e-mail messages.

Telnet: Used to allow remote logins and command execution.

The Session layer is incorrect because this layer creates, manages, and terminates sessions between communicating nodes. NetBIOS and Session Control Protocol (SCP) work at the session layer.

The Presentation layer is incorrect because this layer enables coding and conversion functions for application layer data. The Presentation layer includes graphic image formats, such as Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF).

The Network layer is incorrect because this layer defines the network address or the Internet Protocol (IP) address, which are then used by the routers to make forwarding decisions.

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

References:
Cisco Documentation > Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems

QUESTION 242
A packet is received with a destination IP address of 10.2.16.10. What would the next hop IP address be for this packet?

```
Router# show ip route
<<output omitted>>

D 10.0.0.0 /8 [90/2172515] via 192.168.1.10, 00:00:44, Serial0/0
D 10.1.0.0 /16 [90/2144425] via 192.168.1.10, 00:01:03, Serial0/0
C 192.168.1.0 is directly connected, Serial0/0
C 192.168.4.0 is directly connected, Serial0/1
D 10.2.16.0 /24 [90/2162425] via 192.168.4.2, 00:00:25, Serial0/1
C 192.168.10.0 is directly connected, Serial1/0
D 10.2.32.0 /24 [90/2172425] via 192.168.10.254, 00:00:21, Serial1/0
          90/2172425] via 192.168.1.10, 00:03:33:, Serial0/1
```

A. 192.168.1.10
B. 192.168.4.2
C. 192.168.10.254
D. None; the packet will be dropped.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The packet will be routed to the next hop IP address of 192.168.4.2, since this routing table entry is the most specific match for the remote network. Packets are routed according to the most specific, or "longest," match in the routing table.

The packet in the scenario has a destination IP address of 10.2.16.10, which matches two entries in the routing table.

- 10.0.0.0 /8: this matches based on the /8 mask, where only the first byte has to match. The destination IP address of 10.2.16.10 has a first byte matching 10. If this were the only matching route table entry, it would be selected.

- 10.2.16.0 /24: The first 24 bits of this entry match the first 24 bits of the destination IP address of 10.2.16.10.

Therefore, the 10.2.16.0 /24 entry is selected for routing this packet because it most specifically matches the destination IP address, or has the longest number of matching bits.

The next hops of 192.168.1.10 and 192.168.10.254 will not be used, as these routes are not the most specific matches for the destination IP address of the packet.

It is interesting to note that packets that are destined for the 10.2.32.0 network will be load balanced across both serial 0/0 and serial 0/1 because the cost (2172425) is the same for both paths.

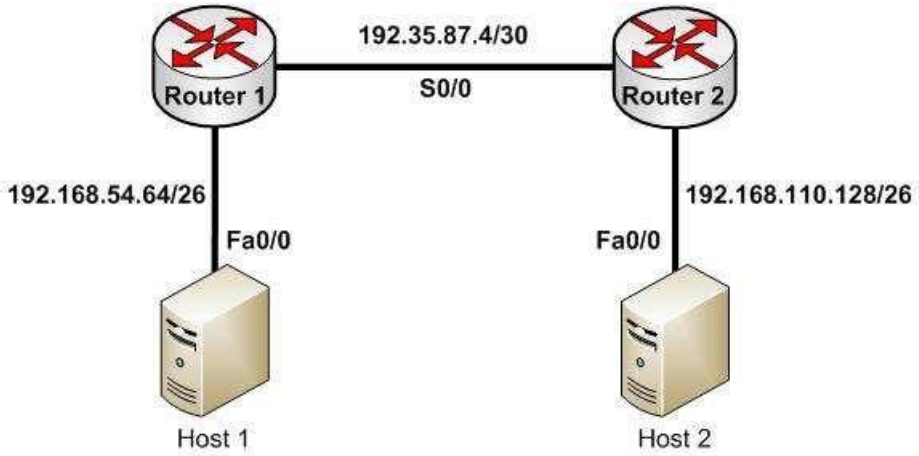
The packet will not be dropped because there is at least one routing table entry that matches the destination IP address of the packet.

To ensure that no packets are dropped, even if there is no matching route in the routing table, a default route could be configured as follows (next hop picked at random for illustration):

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

This configuration would instruct the router to send any packets that do match the existing routes to 192.168.1.1. For example, a packet destined for 201.50.6.8/24 would not match any routes in the table, and would thus be forwarded to 192.168.1.1.

If you understand how routing tables and routing advertisements work, it is relatively simple to describe the contents of a router's routing table without seeing the table directly. To do so, you would view the router's configuration and the configuration of its neighbors using show run, along with a diagram of its network connections. For example, examine the diagram of the two routers shown below along with their respective configurations:




```
hostname router 1                    hostname router 2
router rip                           router rip
network 192.168.54.64                network 192.168.110.128
ip route 0.0.0.0 0.0.0.0 192.35.87.5 <output omitted> <output omitted>
```


Based on this output and diagram, we can reconstruct the contents of the routing table for Router 1 as follows.

```
S*0.0.0.0/0 [1/0] via 192.35.87.5
R 192.168.110.128/26 [120/1] via 192.35.87.5 00:00:22, Serial 0/0
C 192.35.87.4/30 is directly connected, S0/0
C 192.168.54.64/26 is directly connected, Fa0/0
```

It will contain S*0.0.0.0/0 [1/0] via 192.35.87.5 because of the static default route indicated in line 4 of its configuration output.

It will contain R 192.168.110.128/26 [120/1] via 192.35.87.5 00:00:22, Serial 0/0 because Router 2 has a network 192.168.110.128 statement indicating that it will advertise this network to its neighbors.

It will contain the two routes C 192.35.87.4/30 is directly connected, S0/0 and C 192.168.54.64/26 is directly connected, Fa0/0 because all directly connected routes are automatically placed in the table.

Objective:
Routing Fundamentals

Sub-Objective:
Interpret the components of routing table

References:
Cisco > Support > IP > IP Routing > Design > Design TechNotes > Route Selection in Cisco Routers > Document ID: 8651

QUESTION 243
Which three statements are TRUE regarding a Local Area Network (LAN)? (Choose three.)

A. A LAN is 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:
A LAN 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:
Cisco Documentation > Internetworking Technology Handbook > Introduction to LAN Protocols

QUESTION 244
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 protocolD. 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 the client 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:
Cisco > Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 > Part 3: DHCP > Configuring the Cisco IOS DHCP Relay Agent
Cisco > Cisco IOS IP Application Services Command Reference > ip helper-address

QUESTION 245
Which of the following statements are true when discussing link state and distance vector routing protocols? (Choose all that apply.)

A. After convergence, routing advertisements are only triggered by changes in the network with distance vector protocols
B. Packets are routed based upon the shortest path calculated by an algorithm with link state protocols
C. Only one router in an OSPF area can represent the entire topology of the network
D. Distance vector protocols send the entire routing table to a neighbor
E. Distance vector protocols send updates regarding the status of their own links to all routers in the network
F. Link-state protocols place a high demand on router resources running the link-state algorithm
G. Distance vector protocols require a hierarchical IP addressing scheme for optimal functionality
H. Link-state protocols use hello packets and LSAs from other routers to build and maintain the topological database
I. Link-state protocols require a hierarchical IP addressing scheme for optimal functionality.

Correct Answer: BDFHI

Section: (none)
Explanation

Explanation/Reference:
Explanation:
The following statements are true of link-state and distance vector routing protocols:

▪ Packets are routed based upon the shortest path calculated by an algorithm with link state protocols. ▪
Distance vector protocols send the entire routing table to a neighbor.
▪ Link-state protocols place a high demand on router resources running the link-state algorithm.
▪ Link-state protocols use hello packets and LSAs from other routers to build and maintain the topological database. ▪ Link-
state protocols require a hierarchical IP addressing scheme for optimal functionality.

Link state protocols like OSPF use the Shortest Path First algorithm to calculate the shortest path based on a metric called cost, while distance vector protocols like RIP consider only hop count when determining the best route. Running the algorithm places a high demand on router resources. Distance vector protocols are required to send the entire routing table with each update, while link state protocols only send updates when required by changes in the network. Therefore, less traffic is created with link state protocols.

Sending routing advertisements after convergence only when changes occur in the network is a characteristic of link state protocol's not distance vector protocols. With distance vector protocols, updates occur regularly and include the entire routing table.

All routers in an OSPF area can represent the entire topology of the network, not just one.

Distance vector protocols do not send updates regarding the status of their own links to all routers in the network. Updating link status is a characteristic of link state protocols. Distance vector protocols send the entire routing table.

Distance vector protocols do NOT require a hierarchical IP addressing scheme for optimal functionality. Link-state protocols do require this for optimal functionality, as it supports more efficient route aggregation or summarization. This reduces the number of routes in the table and the number of calculations required by the SPF algorithm, thereby lowering router resource demand.

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast distance vector and link-state routing protocols

References:
Cisco>Internetworking Technology Handbook>Routing Basics>Link-State versus Distance Vector

QUESTION 246
In the given exhibit, which combination shows the components of a bridge ID used for Spanning Tree Protocol (STP)?

1

VLAN Number	MAC Address

2

Priority Number	Serial Number

3

Priority Number	MAC Address

4

VLAN Number	Serial Number

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The bridge ID, also known as the switch ID, is used to elect the root bridge in a redundant network topology. The bridge ID has two components:
- Switch's priority number: Configured as 32768 on Cisco switches by default
- Switch's Media Access Control (MAC) address: The burnt-in hardware address of the network interface card (NIC)

The switch with the lowest bridge ID is elected as the root bridge. If the same priority number is configured on two or more switches in the network, the switch with the lowest MAC address will become the root.

Bridge Protocol Data Units (BPDUs) communicate the details of the switch with the lowest bridge ID in the network. The election process for the root bridge takes place every time there is a topology change in the network. A topology change may occur due to the failure of a root bridge or the addition of a new switch in the network. The root bridge originates BPDUs every two seconds, which are propagated by other switches throughout the network. BPDUs are used as keepalives between switches. If a switch stops receiving BPDUs from a neighboring switch for ten intervals (20 seconds), it will assume a designated role for the network segment.

The combinations of the remaining options are incorrect because Virtual LAN (VLAN) numbers and serial numbers are not components of a bridge ID.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Cisco Documentation > Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX > Configuring STP and IEEE 802.1s MST > Understanding the Bridge ID
CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot STP protocols

QUESTION 247
Which of the following commands configures an SNMP host to authenticate a user by username and send clear text notifications, the receipt of which will be acknowledged by the receiver?

A. Router(config)# snmp-server host 192.168.5.5 informs version 3 noauth public
B. Router(config)# snmp-server host 192.168.5.5 traps version 3 auth public
C. Router(config)# snmp-server host 192.168.5.5 informs version 2c public
D. Router(config)# snmp-server host 192.168.5.5 informs version 3 authpriv public

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The command snmp-server host 192.168.5.5 informs version 3 noauth CISCO will configure the host to authenticate a user by username and send clear text notifications. The receiver will then acknowledge receipt of the notification. The keyword informs indicates that an inform message type will be used. Unlike a trap, an inform message is acknowledged by the receiver.

The version 3 keyword indicates that version 3 is in use, which is the ONLY version that supports authentication and encryption. Finally, the noauth keyword specifies authentication by username only and no encryption.

The command snmp-server host 192.168.5.5 traps version 3 auth public configures the host to send traps rather than informs.

The command snmp-server host 192.168.5.5 informs version 2c public specifies version 2c, which only support community string-based authentication.

The command snmp-server host 192.168.5.5 informs version 3 authpriv public specifies the keyword authpriv, which indicates encryption will be used and authentication based on HMAC-MD5 or HMAC-SHA algorithms.

Objective:

Infrastructure Management Sub-
Objective:
Configure and verify device-monitoring protocols

References:
Configuring SNMP Support > Understanding SNMP > SNMP Versions

Cisco IOS Network Management Command Reference > snmp-server engineID local through snmp trap link-status > snmp-server host

QUESTION 248
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/extended range) spanning multiple switches

References:
Cisco > Support > LAN Switching > Virtual LANS / VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Configuring VLAN Trunk Protocol (VTP) > Document ID: 98154
Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25) > Understanding and Configuring VLANs, VTP, and VMPS

QUESTION 249
Which two are NOT features of Cisco NAT implementation? (Choose two.)

A. overload
B. override
C. overrule
D. static NAT
E. dynamic NAT

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Override and overrule are NOT features of Cisco's Network Address Translation (NAT) implementation. NAT translates internal IP address to external IP address and vice versa. NAT is typically used by firewalls or routers.

The following are some of the characteristics of NAT:
- It can act as an address translator between Internet and the local network.
- It conserves IP addresses and simplifies the process of IP address allocation.
- It allows the local network to connect to Internet using unregistered IP addresses.
- It can present only one address for the entire network to the outside world when using dynamic NAT.
- It enhances network security, as it does not disclose internal network addresses to the outside world.

All of the other options are incorrect because they are valid NAT features.

With static NAT, translation mappings are created statically and are placed in the translation tables whether or not there is traffic flowing. In this case, no registered addresses are saved because a registered address is still required for each mapping.

With dynamic NAT, the translation table is populated as the required traffic flows through NAT-enabled devices. In this case, a single address or multiple public addresses can be used multiple times to represent multiple private addresses.

The overload keyword allows the ip nat inside command to translate multiple devices in the internal network to the single address in the IP address pool. This process is also called overloading in that the same public IP address is mapped to all private addresses from inside the network. Since the router performing the NAT overload function will use the unique TCP source port from each host for identification, while mapping all of them to the same public IP address, it is sometimes referred to as Port Address Translation or PAT.

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 variant of this command is given below, which configures NAT to overload on the address assigned to the serial 0 interface:

```
ip nat inside source list 3 interface serial 0 overload
```

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

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

References:
Cisco > Technology Support > IP > IP Routing > Design Technotes > Configuring Network Address Translation: Getting Started > Document ID: 13772 > Quick Start Steps for Configuring and Deploying NAT

QUESTION 250
Which classful protocols perform an automatic summarization of routes when routers send updates across major classful network boundaries? (Choose two.)

A. RIPv1
B. RIPv2
C. IGRP
D. OSPF
E. EIGRP

F. BGPv4

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The classful routing protocols Routing Information Protocol version1 (RIPv1) and Interior Gateway Routing Protocol (IGRP) summarize routes at classful network boundaries. RIPv1 is a standard distance vector protocol that uses hop count as a metric. IGRP is a Cisco Systems proprietary distance vector routing protocol that has a composite metric based on bandwidth, delay, load, reliability, and maximum transmission unit (MTU).

In classless routing protocols RIPv2, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP) and Border Gateway Protocol version 4 (BGPv4), route summarization can be controlled manually at any bit position in the IP address. Classless routing protocols transmit subnet mask along with the routes, and therefore manual summarization may be required at times to keep the routing table size in control.

It should be noted that RIPv2 and EIGRP, although classless protocols, will perform automatic summarization by default unless the no auto-summary command is configured. Once no auto-summary is configured, you can manually configure summarization on any bit position in the IP address. Since you can override autosummarization in both RIPv2 and EIGRP, RIPv1 and IGRP are better answers to this question.

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast interior and exterior routing protocols

References:
Cisco > Articles > Cisco Networking Academy > CCNP 1: Advanced IP Addressing Management

QUESTION 251
You have configured a router as shown in the following output:

```
ip dhcp pool POOLNAME
network 10.2.10.0 255.255.255.0
default-router 10.2.10.254
dns-server 10.6.1.200
!
interface fastethernet0/0
ip nat inside
!
interface serial0/1
ip address 200.14.3.25 255.255.255.252
ip nat outside
!
access-list 1 permit 10.2.10.0 0.0.0.255
!
ip nat pool NATPOOL 205.2.1.1 205.2.1.14 netmask 255.255.255.240
ip nat inside source list 1 pool NATPOOL
```

Hosts on the LAN cannot receive an IP address. What is wrong?

A. The IP address on the serial interface is incorrect.

B. The default-router command in the DHCP pool is incorrect.
C. An IP address needs to be configured on the FastEthernet interface.
D. The NAT pool is not large enough.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An IP address needs to be configured on the FastEthernet interface. Dynamic Host Control Protocol (DHCP) is used to dynamically provide IP network configurations to workstations as they are booted up. DHCP minimizes network administration overload, allowing devices to be added to the network with little or no manual configuration.

The router configuration in the scenario has created a DHCP address pool called POOLNAME. The network statement in the exhibit, network 10.2.10.0 255.255.255.0, identifies the range of IP addresses that the pool will provide to host systems (10.2.10.0 /24). However, a DHCP pool can only provide IP addresses over a subnet to which it is directly connected. Because neither of the interfaces in the exhibit has an IP address on the 10.2.10.0 /24 subnet, the solution is to assign the FastEthernet0/0 interface the IP address specified in the default-router statement, 10.2.10.254 /24.

The IP address on the serial interface has no impact on the DHCP pool.

The default-router statement is correctly providing the IP address that DHCP hosts will use as their default gateway. The problem is not with the default-router statement, but with the lack of a correct IP address assigned to the FastEthernet0/0 interface.

The NAT configuration in the exhibit has no impact on the DHCP pool. If the NAT pool were not large enough, the result would be that some of the hosts would be able to get to the Internet and others would not. For example, the output from the diagram shown below indicates that there are fourteen addresses in the pool (205.2.1.1 to 205.2.1.14). If the network contained 30 computers, only fourteen would be able to use the Internet at the same time because of the number of public addresses in the pool:

```
ip nat pool NATPOOL 205.2.1.1 205.2.1.14 netmask 255.255.255.240
ip nat inside source list 1 pool NATPOOL
```

Objective:
Infrastructure Services Sub-
Objective:
Configure and verify DHCP on a router (excluding static reservations)

References:
Cisco > Support > Cisco IOS Software > Configuring the Cisco IOS DHCP Server > Configuring DHCP Address Pools

QUESTION 252
You manage the EIGRP subnet in your organization. You have enabled EIGRP for IPv6 on all the routers in the EIGRP AS 260 using the following commands on all the routers:

The **ipv6 unicast-routing** command in global configuration mode
The **interface** command in global configuration mode
The **ipv6 enable** command in interface configuration mode
The **ipv6 eigrp** command in interface configuration mode
The **ipv6 router eigrp** command in global configuration mode
The **eigrp router-id** command in global configuration mode

During verification, you discover that EIGRP for IPv6 is not running on the routers.

Which of the following should be done to fix the issue?

A. The ipv6 address command should be executed in interface configuration mode.
B. The ipv6 address command should be executed in router configuration mode.
C. The eigrp router-id command should be executed in interface configuration mode.
D. The eigrp router-id command should be executed in router configuration mode.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The eigrp router-id command should be executed in router configuration mode to fix the issue. This command specifies a fixed router IPv4 address to the router. If this command is missing or incorrectly configured on the router, EIGRP for IPv6 will not run properly.

Another command that you should perform so that EIGRP for IPv6 runs on the routers is the no shutdown command. You should execute this command in interface configuration mode. The no shutdown command is necessary because all the interfaces with EIGRP for IPv6 enabled on them are in a shutdown state by default.

A sample configuration to implement EIGRP for IPv6 on a router is as follows:

```
Rtr63(config)# ipv6 unicast-routing
Rtr63(config) # interface Fa0/1
Rtr63(config-if) # ipv6 enable
Rtr63(config-if) # ipv6 eigrp 260
Rtr63(config-if)# no shutdown
Rtr63(config-if) # exit
Rtr63(config)# ipv6 router eigrp 260
Rtr63(config-rtr)# eigrp router-id 1.1.1.1
```


The two options stating that the ipv6 address command should be executed on the routers are incorrect. EIGRP for IPv6 can be configured on router interfaces without explicitly specifying a global unicast IPv6 address. If you specify the ipv6 enable command, as in this scenario, then the IPv6 address command is not required.

The option stating that the eigrp router-id command should be executed in interface configuration mode is incorrect. This command should be executed in router configuration mode instead of interface or global configuration modes.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco IPv6 Implementation Guide, Release 15.2M&T > Implementing EIGRP for IPv6 > How to Implement EIGRP for IPv6 > Enabling EIGRP for IPv6 on an Interface

QUESTION 253

You have multiple departments sharing a common network. You are concerned about network traffic from one department reaching another department.

What would be a solution for isolating the departments? (Choose all that apply.)

A. Configure separate VLANs for each department.
B. Assign a unique VTP domain for each department.
C. Put each department in a separate collision domain.
D. Configure trunk links between departmental switches.
E. Configure separate subnets for each department

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You could either configure separate VLANs for each department or configure separate subnets for each department. Either approach has the effect of restricting each department's traffic to its local subnet or VLAN, unless you configure and allow inter-VLAN routing.

VLANs logically divide a switched network into multiple independent broadcast domains. Broadcast traffic within one VLAN will never be sent to hosts in other VLANs. In this respect, VLANs operate exactly as subnets do. The only way for hosts in different VLANs to communicate is through a router or multilayer switch configured to perform inter-VLAN routing between the VLANs.

The VLAN Trunking Protocol (VTP) is used to synchronize VLAN databases across multiple switches, and is not a method for isolating departmental traffic.

Collision domains cannot be used to isolate traffic between departments. Multiple departments cannot share a collision domain when using switches. Every port on a switch is a separate collision domain, which allows the switch to forward more than one frame at a time. This also reduces collisions, since each host is therefore in a separate collision domain. The switch processes data based only on MAC addresses, and has no knowledge of which host is in which IP subnet or department.

Trunk links are used to connect switches to other switches and to routers for the purpose of carrying traffic from multiple VLANs, and are not a method of isolating traffic between different departments.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco > Internetwork Design Guide > Designing Switched LAN Internetworks > Benefits of VLANs

QUESTION 254
Which of the following is NOT a dynamic table maintained by a router running the EIGRP routing protocol?

A. topology table
B. CAM table
C. routing table
D. neighbor table

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
All are tables maintained by a router running the EIGRP routing protocol except a Content Addressable Memory (CAM) table. This table is only present on a switch. It is used to maintain the two MAC addresses involved in a conversation between computers so that the conversation can be routed once and then switched thereafter which is a much faster process.

EIGRP maintains three dynamic tables in RAM:
- Neighbor table, which is a list of all neighboring EIGRP routers on shared subnets
- Topology table, which contains all discovered network paths in the internetwork
- Routing table, which contains the best path (based on lowest metric) to each destination

Objective:
Routing Fundamentals

Sub-Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:
Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > Enhanced Interior Gateway Routing Protocol > Document ID: 16406 > Feasible Distance, Reported Distance, and Feasible Successor
CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 10: EIGRP, pp. 392-395.

QUESTION 255
Your network consists of one HSRP group of six routers. All of the routers are functioning properly. The network has been stable for several days.

In which HSRP state are most of the routers?

A. Learn
B. Listen
C. Standby
D. Active

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
If all of the routers in the Hot Standby Routing Protocol (HSRP) group are functioning properly, then most of the routers in the group are in the listen state. Four routers will be in the listen state, one router will be in the standby state, and one router will be in the active state.

HSRP is used by a group of routers to create the appearance of a virtual router with which end stations can communicate in the event that the default gateway becomes unavailable. The active router is responsible for forwarding packets that are sent to the virtual router. The standby router is responsible for assuming the role of active router should the active router fail or become unavailable. All other HSRP routers monitor the hello messages sent by the active and standby routers. Should the active and standby routers both become unavailable, the HSRP router with the highest priority is elected to become the active router by default. For routers with equal priority values, the router with the highest IP address becomes the active router.

HSRP routers can exist in one of the following six states:
- Initial
- Learn
- Listen
- Speak
- Standby
- Active

All HSRP routers start in the initial state. A router in the learn state is waiting for its first hello message from the active router so that it can learn the virtual router's IP address. When the hello message is received and the virtual router's IP address is discovered, the HSRP router is in the listen state. A router in the listen state listens for hello messages from the active and standby routers. If an election for a new active router and a new standby router is required, then an HSRP router will enter the speak state and begin transmitting hello messages. The standby state is reserved for the standby router, and the active state is reserved for the active router. Only routers in speak, standby, and active states will transmit hello packets.

Objective:
Infrastructure Services Sub-
Objective:
Configure, verify, and troubleshoot basic HSRP

References:
Cisco > Home > Technology Support > IP > IP Application Services > Design > Design Technotes > Hot Standby Router Protocol Features and Functionality
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

QUESTION 256
What is the default Administrative Distance (AD) value for an Enhanced Interior Gateway Routing Protocol (EIGRP) summary route?

A. 1
B. 5
C. 90
D. 20

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The default Administrative Distance (AD) value for an Enhanced Interior Gateway Routing Protocol (EIGRP) summary route is 5. The following table shows the AD values for different protocols and their IP routes:

IP Route	Default AD value
Connected interface	0
Static route directed to an connected interface	0
Static route directed to an IP address	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP) route	20
Internal Enhanced Interior Gateway Routing Protocol (EIGRP) route	90
Interior Gateway Routing Protocol (IGRP) route	100
Open Shortest Path First (OSPF) route	110
Intermediate System-to-Intermediate System (IS-IS) route	115
Routing Information Protocol (RIP) route	120
Exterior Gateway Protocol (EGP) route	140
On Demand Routing (ODR)	160
External Enhanced Interior Gateway Routing Protocol (EIGRP) route	170
Internal Border Gateway Protocol (BGP) route	200
Unknown origin routes	255

The option 1 is incorrect because this is the default AD value for static routes.

The option 90 is incorrect because this is the default AD value for internal EIGRP routes.

The option 20 is incorrect because this is the default AD value for external BGP routes.

Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast interior and exterior routing protocols

References:

QUESTION 257
You are the network administrator for your company. The network at the company's office is due to be upgraded, and you have been assigned the responsibility of identifying the requirements for designing the network. You need to provide network connectivity to 200 client computers that will reside in the same sub network, and each client computer must be allocated dedicated bandwidth.

Which device should you use to accomplish the task?

A. router
B. hub

C. switch
D. firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should use a switch to accomplish the task in this scenario. A switch is used to provide dedicated bandwidth to each node by eliminating the possibility of collisions on the switch port where the node resides. Switches work at Layer 2 in the Open System Interconnection (OSI) model and perform the function of separating collision domains. When a node resides in its own collision domain, the possibility of collisions (which slow throughput due to the subsequent but necessary retransmission) is eliminated. The advantage of using a switch instead of a hub is that a switch provides dedicated bandwidth to each client, while all connected clients share the bandwidth on a hub.

A router will not be a suitable device in this scenario. Routers are Network layer devices that are used to separate broadcast domains and connect two or more different subnets or network types. There is only a single subnet in the scenario so a router is not required.

A hub will not be a suitable device in this scenario. Hubs are Physical layer (Layer 1) devices that are used to connect clients to the network. A hub simply broadcasts data to all its ports; it does not create separate collision domains. All clients connected to a hub are a member of a single collision domain. In a scenario where a number of devices connected to a hub are experiencing network slowdowns, especially when using network-based applications, replacing the hub with a switch is almost always the best solution.

A firewall will not be a suitable device in this scenario. A firewall is a device used to secure the network against unauthorized intrusions and malicious attacks.

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

References:
Cisco Documentation > Internetwork Design Guide > Internetworking Design Basics

QUESTION 258
The following is a partial output of the show interfaces command:

```
Serial 0 is up, 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 up, line protocol is down statement signify in the output? (Choose all that apply.)

A. the shutdown interface command is present in the router configuration

B. a cable is unplugged
C. the interface is displaying normal operation
D. there are no problems with physical connectivity
E. there is a configuration problem in the local or remote router

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Serial 0 is up, line protocol is down statement in the output signifies the following:
- There are no problems with the physical connectivity.
- There is a configuration problem in the local or remote router.
- The remote router might not be sending the keep-alives.
- There may be a problem with the leased lines such as line noise and a malfunctioning switch.
- There is an incorrect configuration of the CSU/DSU, which can cause timing issues on the cable.
- The local or remote CSU/DSU might have failed.

The option stating that the shutdown interface command is present in the router configuration is incorrect because if the shutdown interface command is present in the router configuration, the message displayed would be Serial 0 is administratively down, line protocol is down.

The option stating that a cable is unplugged is incorrect because that would be indicated by Serial 0 is down, line protocol is down. Physical problems such as a bad cable or cable unplugged are addressed in the first part of the output (serial0 is up/down).

The option stating that the message refers to normal operation of the interface is incorrect because the line protocol is shown as down, which indicates a problem.

Objective:
Routing Fundamentals Sub-
Objective:
Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

QUESTION 259
Which Cisco Internetwork Operating System (IOS) command is used to view information about Open Shortest Path First (OSPF) routing processes?

A. show ip ospf database
B. show ip ospf statistics

C. show ip ospf
D. show ip ospf traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The show ip ospf command is used to view information about the OSPF routing processes. It does so by displaying the collection of link states present in the database. The syntax of the command is as follows:

Router# show ip ospf [process-id]

The process-id parameter of the command specifies the process ID. The output of the command is as follows:

```
Router# show ip ospf

Routing Process "ospf 203" with ID 21.0.0.1 and Domain ID 21.20.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 10 secs, Hold time between two SPFs 20 secs
Minimum LSA interval 10 secs. Minimum LSA arrival 5 secs
LSA group pacing timer 200secs
Interface flood pacing timer 110 msecs
Retransmission pacing timer 110 msecs
Number of external LSA 1. Checksum Sum 0x0
Number of opaque AS LSA 1. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 3. 1 normal 0 stub 1 nssa
External flood list length 0

Area BACKBONE(0)
Number of interfaces in this area is 4
Area has message digest authentication
SPF algorithm executed 6 times
Area ranges are
Number of LSA 3. Checksum Sum 0x29BEB
Number of opaque link LSA 1. Checksum Sum 0x0
Number of DCbitless LSA 3
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

The show ip ospf database command is incorrect because this command is used to view the OSPF database for a specific router.

The show ip ospf statistics command is incorrect because this command is no longer valid in IOS version 12.4.

The show ip ospf traffic command is incorrect because this command is no longer valid in IOS version 12.4.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

QUESTION 260
What is the term used for the Ethernet communication mechanism by which hosts can send and receive data simultaneously?

A. full-duplex
B. multiplex
C. half-duplex
D. duplex

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Full-duplex communication occurs when workstations can send and receive data simultaneously. To support full-duplex communication, both communicating hosts should be configured to transmit in full-duplex mode. With the use of full-duplex communication, the bandwidth can effectively be doubled. Hubs are not capable of handling full-duplex communication, and you need a dedicated switch port to allow full-duplex communication.

Half-duplex is the term used for the Ethernet communication mechanism when hosts can send or receive data, but not simultaneously.

It is important that the switch and the device connected to the switch have the same duplex and speed settings, or there will intermittent connectivity and loss of connection. To verify the duplex and speed settings on a switch, execute the show interfaces command, specifying the interface and the setting can be verified (as shown in line 8 in the output below):

```
switch# show interface fastethernet 0/3
```

```
Fast Ethernet 0/3 is down, line protocol is down (not connect)

Hardware is Fast Ethernet, address is 00e0.1e3e.2a02

MTU 1500 bytes, BW 10000 Kbit, DLY 100 usec, rely 1/255, tx load
1/255, rxload 1/255

Encapsulation ARPA, loopback not set,

Keepalive set (10 sec)

Half-duplex, 100Mb/s

ARP type: ARPA, ARP Timeout 04:00:00
```

From the output above it can be seen that the switch interface is set for half duplex and the speed is set for 100Mb/s. This means that if the host connected to this switch port is set differently, for example set to 1 Gb/s because it has a 1 Gb NIC, the host and the switch interface will not communicate and the host will not be able to connect to the network.

Multiplex is the term used when multiple signals are combined to be transferred via one signal.

Duplex implies that there are two communication paths. However, the term does not specify the required functionality, which is full duplex.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Describe and verify switching concepts

References:
Cisco > Support > Technology Support > LAN Switching > Ethernet > Design > Design Technotes > Configuring and Troubleshooting Ethernet 10/100/1000Mb Half/
Full Duplex Auto-Negotiation > Document ID: 10561

QUESTION 261
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-telcoFas
0/0 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 Intrfce: The protocol which the connectivity media uses.
Holdtme: 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:
Cisco > Cisco IOS Network Command Reference, Release 12.4 > show cdp neighbors

QUESTION 262
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.

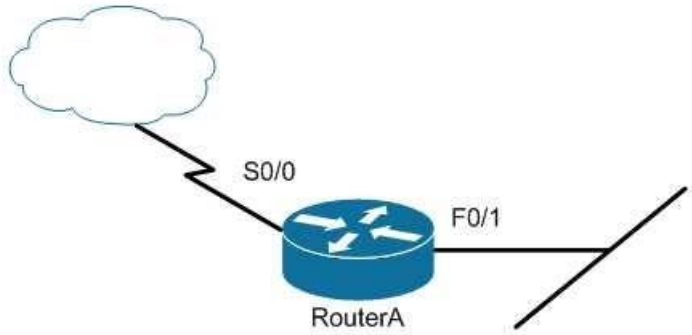
A hub does not split the network into separate broadcast domains. A hub regenerates signal when it passes through its ports, which means that it acts as a repeater and port concentrator only. Hubs and repeaters are Layer 1 devices that can be used to enlarge the area covered by a single LAN segment, 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:

Cisco Documentation > Internetworking Case Studies > LAN Switching

QUESTION 263
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 shutdown command 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 encapsulation type 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 not be 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:
Cisco > Support > Administrative Commands > shutdown

QUESTION 264
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 in privileged 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 Management Sub-
Objective:
Perform device maintenance

References:
Cisco > Support > IOS and Configuration Basics > Saving Configuration Changes

QUESTION 265
You have executed the following commands on a switch:

```
Switch64(config)# interface range gigabitethernet2/0/1 -2
Switch64(config-if-range)# switchport mode access
Switch64(config-if-range)# switchport access vlan 10
Switch64(config-if-range)# channel-group 5 mode auto
```

In which of the following situations will Switch64 create an Etherchannel?

A. If the other switch is set for desirable mode
B. If the other switch is set for auto mode
C. If the other switch is set for on mode

D. If the other switch is set for passive mode

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Etherchannel will be created if the other end is set to desirable mode. The configuration shown in the example is using Port Aggregation protocol (PAGP). This protocol has two settings: desirable and auto. Two ends will negotiate and will only create an Etherchannel under two conditions: if one end is set to auto and the other end is set to desirable, or if both ends are set for desirable.

It will not form an Etherchannel if the other end is set to auto mode. When both ends are set to auto mode, an Etherchannel will not form.

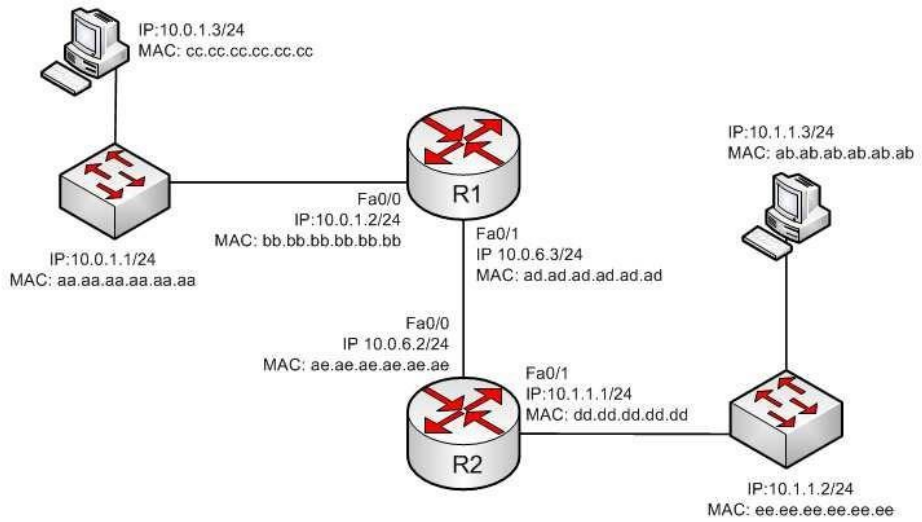
It will not form an Etherchannel if the other end is set to on mode. On mode disables negotiation of any kind, which will prevent an Etherchannel from forming unless the other end is also set for on.

It will not form an Etherchannel if the other end is set to passive mode. Passive is a setting used in Link Aggregation Protocol (LACP). The two protocols are not compatible.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel

References:
Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE > Chapter: Configuring EtherChannels

QUESTION 266
The workstation at 10.0.1.3 sends a packet to the workstation at 10.1.1.3.



When the packet leaves the R2 router, what addresses will be located in the header? (Choose two.)

A. Source MAC bb.bb.bb.bb.bb.bb Dest MAC ab.ab.ab.ab.ab.ab
B. Source MAC dd.dd.dd.dd.dd.dd Dest MAC ab.ab.ab.ab.ab.ab
C. Source MAC ee.ee.ee.ee.ee.ee Dest MAC ab.ab.ab.ab.ab.ab
D. Source IP 10.0.1.3 Dest IP 10.1.1.3
E. Source IP 10.0.1.1 Dest IP 10.1.1.2
F. Source IP 10.0.1.2 Dest IP 10.1.1.3
G. Source IP 10.0.1.1 Dest IP 10.1.1.3

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When the packet leaves the R2 router, the addresses that will be located in the header are:

Source MAC dd.dd.dd.dd.dd.dd
Dest MAC ab.ab.ab.ab.ab.ab

Source IP 10.0.1.3 Dest
IP 10.1.1.3

If we executed the ipconfig/all command on the computer located at 10.1.1.3/24, it would look somewhat like what is shown below. The router interface (10.1.1.1/24) would use an ARP broadcast to determine the MAC address associated with the IP address 10.1.1.3/24 and it would be returned as ab.ab.ab.ab.ab.ab. The router interface would then encapsulate the packet in a frame addressed to ab.ab.ab.ab.ab.ab.

```
Connection-specific DNS Suffix : acme.com
Description . . . . . .: Broadcom NetXtreme 57xx Gigabit Controller

Physical Address. . . . . : AB-AB-AB-AB-AB-AB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . : fe80::ada3:8b73:a66e:6bc0%10(Preferred)
IPv4 Address. . . . . : 10.1.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, October 14, 2011 12:42:05 PM
Lease Expires . . . . . .: Thursday, October 20, 2011 12:44:20 AM
Default Gateway . . . . . : 10.1.1.1
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
```


The source and destination IP address 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 R2, the source MAC address will be that of R2, and the destination will be that of the workstation at 10.1.1.3. 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 the packet to its default gateway at 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:
Cisco > IOS Technology Handbook > Routing Basics

QUESTION 267
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:

QUESTION 268
What is the significance of the 1 in the following configuration?

```
router(config)# router eigrp 1
```

A. It is the process ID for EIGRP and is locally significant to this router.

B. It is the process ID for EIGRP and must be the same on all EIGRP routers.
C. It is the AS number for EIGRP and is locally significant to this router.
D. It is the AS number for EIGRP and must be the same on all EIGRP routers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Enhanced Interior Gateway Routing Protocol (EIGRP) configuration requires the specification of an Autonomous System (AS) number with the router eigrp command. Any number can be chosen, but it must match on all EIGRP routers in the domain. This value may appear to be is similar to one used in enabling OSPF, which demands a process ID number but that value is locally significant to each router and need not match on each router.

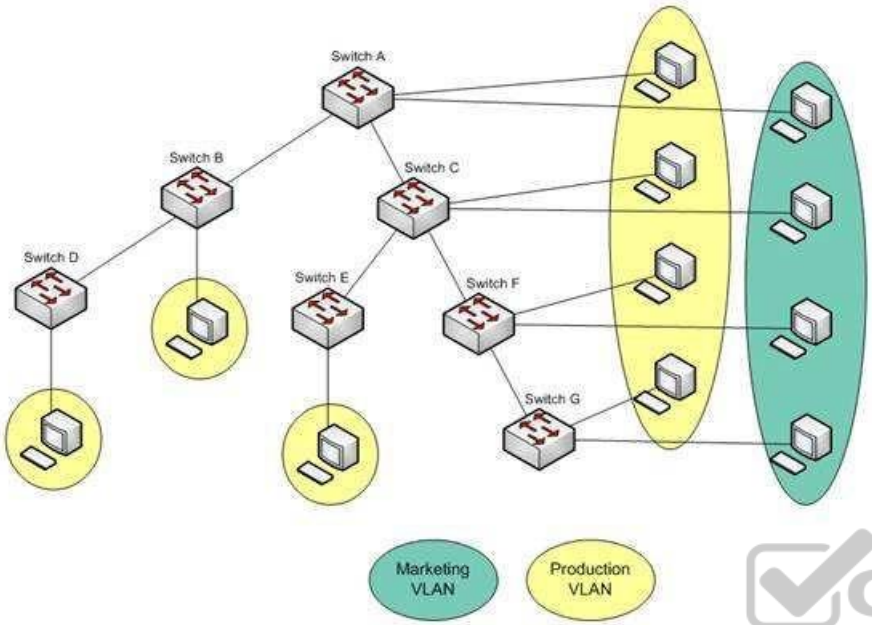
The syntax of this command is router eigrp [autonomous-system]. Therefore, the 1 in the example indicates an Autonomous System (AS) number, not a process ID.

The Autonomous System (AS) number is not locally significant to each router, and must match on all EIGRP routers.

Objective:
Routing Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

QUESTION 269
You are a network administrator for your organization. Your organization has two Virtual LANs (VLANs) 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, while switches B, D, and E have user machines connected for the Production VLAN only. (Click the Exhibit(s) button to view the network diagram.)



To reduce broadcast traffic on the network, you want to ensure that broadcasts from the Marketing VLAN are flooded only to those switches that have Marketing VLAN users.

Which Cisco switch feature should you use to achieve the objective?

A. PVST
B. RSTP
C. VTP Pruning
D. Dynamic VLANs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The VLAN Trunking Protocol (VTP) pruning feature of Cisco VTP allows switches to dynamically delete or add VLANs to a trunk. It restricts unnecessary traffic, such as broadcasts, to only those switches that have user machines connected for a particular VLAN. It is not required to flood a frame to a neighboring switch if that switch does not have any active ports in the source VLAN. A trunk can also be manually configured with its allowed VLANs, as an alternative to VTP pruning.

All other options are incorrect because none of these features can be used to achieve the objective in this scenario.

The Per-VLAN Spanning Tree (PVST) feature allows a separate instance of Spanning Tree Protocol (STP) per VLAN. Each VLAN will have its own root switch and, within each VLAN, STP will run and remove loops for that particular VLAN.

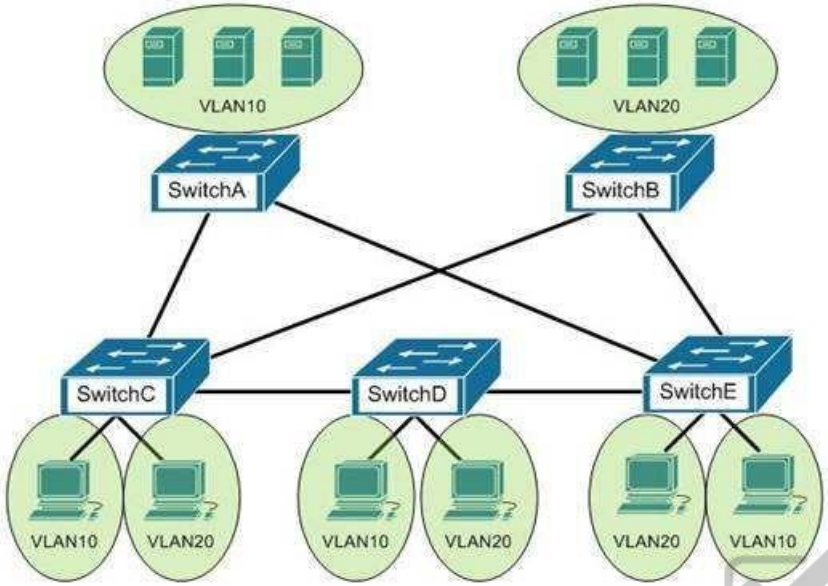
Rapid Spanning Tree Protocol (RSTP) is an Institute of Electrical and Electronics Engineers (IEEE) standard. It reduces high convergence time that was previously required in STP implementations. It is interoperable with STP (802.1d).

With dynamic VLANs, the switch automatically assigns a switch port to a VLAN using information from the user machine, such as its Media Access Control (MAC) address or IP address. The switch then verifies information with a VLAN Membership Policy Server (VMPS) that contains a mapping of user machine information to VLANs.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:
Cisco > Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.1E > Configuring VTP
Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design TechNotes > How LAN Switches Work > Document ID: 10607

QUESTION 270
You are the switch administrator for InterConn. The network is physically wired as shown in the diagram. You are planning the configuration of STP. The majority of network traffic runs between the hosts and servers within each VLAN.



You would like to designate the root bridges for VLANS 10 and 20. Which switches should you designate as the root bridges?

A. Switch A for VLAN 10 and Switch E for VLAN 20
B. Switch A for VLAN 10 and Switch B for VLAN 20
C. Switch A for VLAN 10 and Switch C for VLAN 20
D. Switch D for VLAN 10 and Switch B for VLAN 20
E. Switch E for VLAN 10 and Switch A for VLAN 20
F. Switch B for VLAN 10 and Switch E for VLAN 20

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You should designate Switch A for VLAN 10 and Switch B for VLAN 20. The STP root bridge for a particular VLAN should be placed as close as possible to the center of the VLAN. If the majority of network traffic is between the hosts and servers within each VLAN, and the servers are grouped into a server farm, then the

switch that all hosts will be sending their data to is the ideal choice for the STP root. Cisco's default implementation of STP is called Per-VLAN Spanning Tree (or PVST), which allows individual tuning of the spanning tree within each VLAN. Switch A can be configured as the root bridge for VLAN 10, and Switch B can be configured as the root bridge for VLAN 20, resulting in optimized traffic flow for both.

None of the other switches is in the traffic flow of all data headed towards the VLAN 20 or VLAN 10 server farms, so they would not be good choices for the root bridge for either VLAN. Care should be taken when adding any switch to the network. The addition of an older, slower switch could cause inefficient data paths if the old switch should become the root bridge.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot STP protocols

References:
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and TechNotes > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

QUESTION 271
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:
Home > Support > Using the Command-Line Interface in Cisco IOS Software

QUESTION 272
What command produced the following output?

```
Routing Protocol is "igrp 120"
Sending updates every 90 seconds, next due in 44 seconds
Invalid after 270 seconds, hold down 280, flushed after 630
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
IGRP maximum hopcount 100
IGRP maximum metric variance 1
Redistributing: igrp 109
Routing for Networks:
172.160.74.0
Routing Information Sources:
Gateway Distance Last Update
172.160.74.18 100 0:56:41
172.160.74.19 100 6d19
172.160.74.22 100 0:25:41
172.160.74.20 100 0:01:04
172.160.74.30 100 0:02:29
Distance: (default is 100)
Routing Protocol is "bgp 18"
Sending updates every 60 seconds, next due in 0 seconds
Outgoing update filter list for all interfaces is 1
Incoming update filter list for all interfaces is not set
Redistributing: igrp 109
IGP synchronization is disabled
Automatic route summarization is enabled
Neighbor(s):
Address FiltIn FiltOut DistIn DistOut Weight RouteMap
192.109.211.17 1
192.109.213.89 1
198.6.255.13 1
172.161.72.18 1
172.161.72.19
172.161.84.17 1
Routing for Networks:
192.108.209.0
192.108.211.0
198.6.254.0
Routing Information Sources:
Gateway Distance Last Update
172.161.72.19 20 0:05:28
Distance: external 20 internal 200 local 200
```

A. show ip process

B. show ip route

C. show ip protocols
D. show ip routing process

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. It has the following syntax:

Router# show ip protocols

This command does not have any parameters.

The output was not produced by the command show ip process or the show ip routing process. The show ip routing process and show ip process commands are incorrect because these are not valid Cisco IOS commands.

The output was not produced by the command show ip route. The show ip route command is is used to view the current state of the routing table. An example of the output is shown below.

```
router>show ip route

Codes: C - connected O - OSPF i - IS-IS

S - static IA - inter area L1 - level-1

B - BGP E1 - external type 1 L2 - level-2

E2 - external type 2

* - candidate default

m - route's metric

w - route's weight

S 0.0.0.0/0 directly connected to null 0

C 6.1.1.64/28 directly connected to ethernet 1

C 6.1.1.80/28 directly connected to ethernet 2

C 6.1.1.96/28 directly connected to ethernet 3

C 6.1.1.112/28 directly connected to ethernet 4

S 11.1.0.0/16 via 10.5.0.1 [w:0 m:0]

C 11.5.0.0/16 directly connected to ethernet 0

S 127.0.0.0/8 directly connected to null 0
```


Objective:
Routing Fundamentals Sub-
Objective:
Compare and contrast distance vector and link-state routing protocols

References:
CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 11: Troubleshooting Routing Protocols, pp. 410-413.

QUESTION 273
Which of the following statements are NOT part of the guidelines for configuring VLAN Trunking Protocol (VTP) to ensure that VLAN information is distributed to all Cisco switches in the network? (Choose all that apply.)

A. The VTP version must be the same on all switches in a VTP domain.

B. The configuration revision number must be configured identically on all switches in a VTP domain.
C. The VTP password must be the same on all switches in a VTP domain.
D. The VTP domain name must be the same on all switches in a VTP domain.
E. VLANs configured on clients should exist on the server switch.
F. The switch(s) that will share VLAN information is(are) operating in VTP server mode
G. The switches must be configured to use the same method of VLAN tagging
H. The switches must be connected with trunk links

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
For all switches in a VTP domain, the VTP version, VTP password, and VTP domain name must be the same. Moreover, switches that will share VLAN information must be operating in VTP server mode, must be using the same VLAN tagging method (either 802.1q or ISL), and must be connected with trunk links.

Many of these settings can be verified by using the show vtp status command. By viewing the output of the command on two switches that are not sharing information, inconsistencies that prevent the sharing of VLAN information can be identified. Consider the output from the two switches below:

```
Switch60# show vtp status              Switch62# show vtp status
VTP Version : 2                        VTP Version : 2
Configuration Revision : 62            Configuration Revision : 62
Max VLAN support locally : 1005        Max VLANs support locally : 1005
Number of existing VLANs : 24          Number of existing VLANs : 24
VTP Operating Mode : Server            VTP Operating Mode : Client
VTP Domain Name : Corporate            VTP Domain Name : Corp
VTP Pruning Mode : Enabled             VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled                 VTP V2 Mode : Disabled
VTP Traps Generation : Disabled        VTP Traps Generation : Disabled

Switch61# show vtp status              Switch63# show vtp status
VTP Version : 2                        VTP Version : 2
Configuration Revision : 62            Configuration Revision : 63
Max VLAN support locally : 1005        Max VLAN support locally : 1005
Number of existing VLANs : 24          Number of existing VLANs : 24
VTP Operating Mode : Transparent       VTP Operating Mode : Client
VTP Domain Name : Corporate            VTP Domain Name : Corporate
VTP Pruning Mode : Enabled             VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled                 VTP V2 Mode : Disabled
VTP Traps Generation : Disabled        VTP Traps Generation : Disabled
```

Based on the output for the four switches, you should NOT expect Switch62 to exchange VLAN information with the other switches because the VTP domain names do not match. Line 6 shows that Swicth62 is set to Corp and the others are set to Corporate. The command to set the VTP domain name is:

Switch62(config)#vtp domain corporate

Switch62 is operating in Client mode, which means it will accept VLAN changes sent by switches operating in Server mode once the domain name mismatch is corrected. It will both process them and forward them, but will not allow VLAN changes to be made locally, and it will not save any of the VLAN information in NVRAM (line 5). The command to place a switch into Client mode is:

Switch62(config)#vtp mode client

Switch60 is operating in Server mode and will allow changes to be made locally, will send those changes to other switches, and WILL save all changes (both learned and made locally) in NVRAM, as shown by line 5. The command to place a switch into Server mode is:

Switch62(config)#vtp mode server

Switch61 is operating in Transparent mode. It will allow changes to be made locally and WILL save all changes made locally in NVRAM, but will NOT send those changes to other switches, as shown in line 5. It will accept and pass along VTP changes from switches operating in Server mode, but will not save those changes in NVRAM. The command to place a switch in Transparent mode is:

Switch62(config)#vtp mode transparent

Switch63 will ignore any information it receives from the other switches, even though the domain name matches, because it has a higher configuration revision number (63) than the other switches. These revision numbers are used by the switches to prevent unnecessary processing of changes that have already been received.

VTP is used to synchronize Virtual Local Area Network (VLAN) databases across switches. VTP server switches can be used to add, delete, or rename VLANs, which are then synchronized over the network with VTP client switches. This allows a network administrator to create a VLAN once, as opposed to having to create it individually on every switch on the network. The password is used to validate the source of the VTP advertisements sent between the switches in the VTP domain.

The option stating that the configuration revision number must be configured identically on all switches in a VTP domain is incorrect. The configuration number cannot be directly configured, but is instead synchronized during VTP updates.

The option stating that VLANs configured on clients should exist on the server switch is incorrect. VTP clients do not allow local VLAN configuration, and can only receive VLANs via VTP synchronization over the network.

Objective:
LAN Switching Fundamentals Sub-
Objective:
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

https://vceplus.com/