

200-301

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

200-301



Website: <https://vceplus.com>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

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.



<https://vceplus.com/>

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 is NOT a valid range for private IP addresses?

- A. 10.0.0.0 - 10.255.255.255
- B. 172.16.0.0 - 172.31.255.255
- C. 192.168.0.0 - 192.168.255.255
- D. 192.255.255.255-193.0.0.0

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Explanation:

The range 192.255.255.255 - 193.0.0.0 is a valid public IP address range, not a private IP address range.

The Internet Assigned Numbers Authority (IANA) has reserved the following three ranges for private Internet use:

10.0.0.0 - 10.255.255.255 (10.0.0.0/8)

172.16.0.0 - 172.31.255.255 (172.16.0.0/12)

192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

The Internet Assigned Numbers Authority (IANA) manages and distributes global public IP addresses. IANA also performs DNS root zone management. IANA operates with the help of International Engineering Task Force (IETF) and RFC Editor to manage IP address allocation and DNS root zone management. There are Regional Internet Registries (RIRs) through which IANA allocates local registrations of IP addresses to different regions of the world. Each RIR handles a specific region of the world.

Objective:

Network Fundamentals Sub-

Objective:

Describe the need for private IPv4 addressing

References:

<http://www.ietf.org/rfc/rfc1918.txt>

<http://www.iana.org/>

QUESTION 3

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:

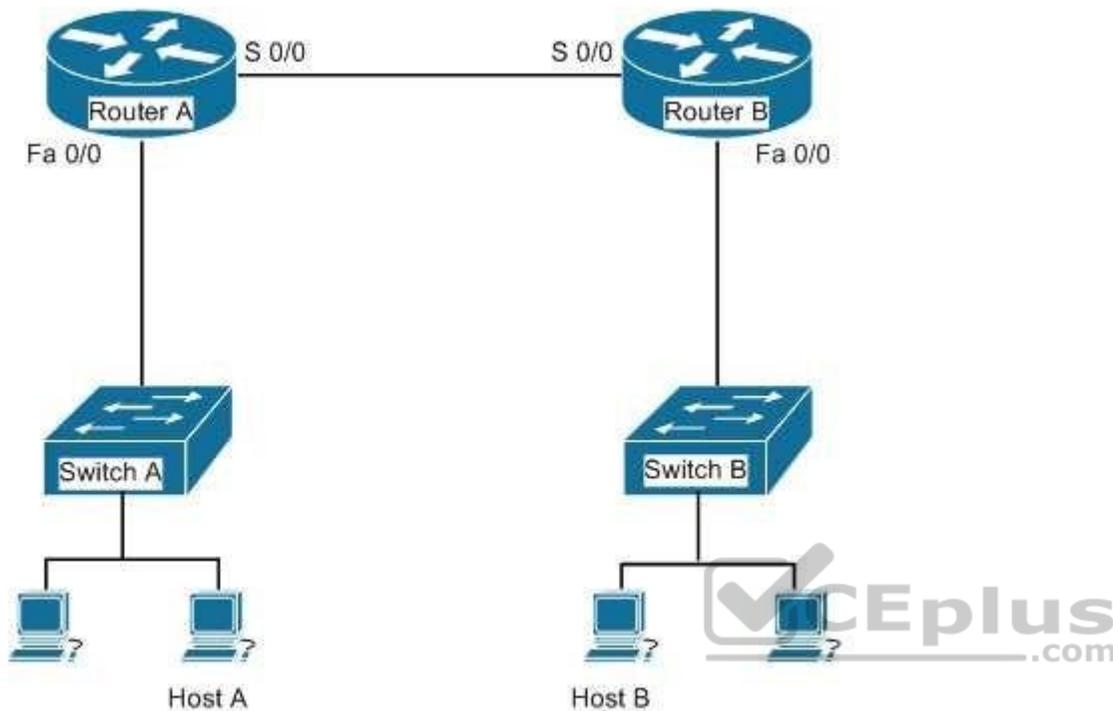
Configure, verify, and troubleshoot STP protocols

References:

[Cisco Home > Support > Technology Support > LAN Switching](#)

QUESTION 4

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

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 5

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

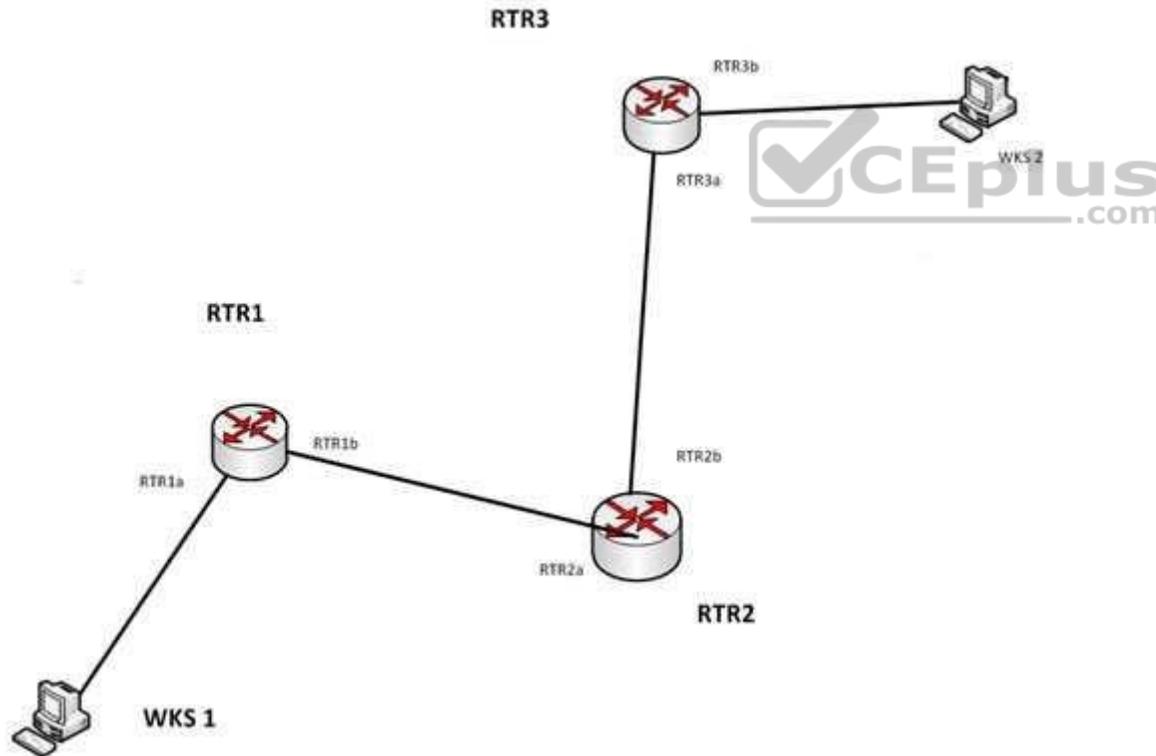
Explanation/Reference:

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 6

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 7

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 8

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 9

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 10

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 11

What command would be used to verify trusted DHCP ports?



- A. `show mls qos`
- B. `show ip dhcp snooping`
- C. `show ip trust`
- D. `show ip arp trust`

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The command `show ip dhcp snooping` is used to verify trusted DHCP ports. This command is used to verify which ports are intended to have DHCP servers connected to them.

DHCP snooping creates an IP address to MAC address database that is used by Dynamic ARP Inspection (DAI) to validate ARP packets. It compares the MAC address and IP address in ARP packets, and only permits the traffic if the addresses match. This eliminates attackers that are spoofing MAC addresses.

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 snooping can be used to determine what ports are able to send DHCP server packets, such as DHCP OFFER, DHCP ACK, and DHCP NAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

MLS QOS has no bearing on DHCP services, so show mls qos is not correct.

The other commands are incorrect because they have invalid syntax.

Objective:

Infrastructure Security Sub-

Objective:

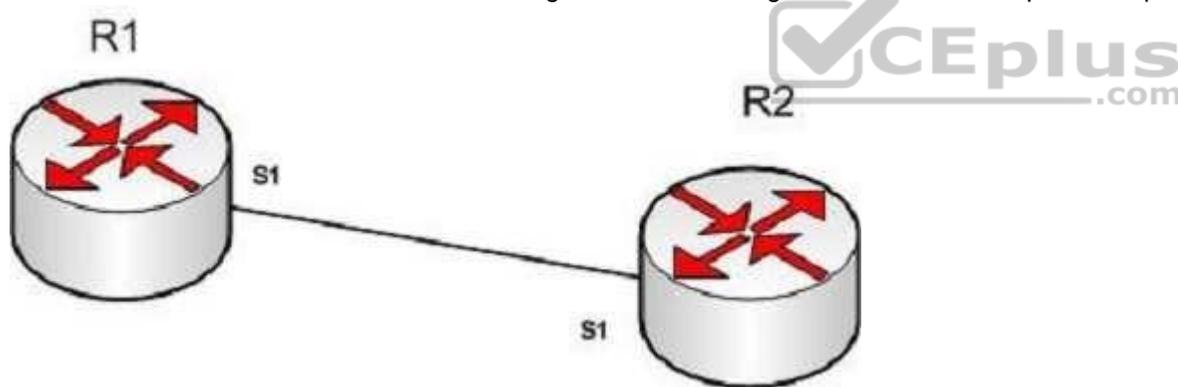
Describe common access layer threat mitigation techniques

References:

[Cisco > Cisco IOS IP Addressing Services Command Reference > DHCP Commands > show ip dhcp snooping](#)

QUESTION 12

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:

Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services, Release 12.3>IP Addressing and Services Commands: idle through ip local-proxyarp>ip host

QUESTION 13

You network team is exploring the use of switch stacking.

Which of the following statements is NOT true of switch stacking?

A. The master switch is the only switch with full access to the interconnect bandwidth

- B. Switches are connected with special cable
- C. The stack has a single IP address
- D. Up to nine switches can be added to the stack

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

All switches in the stack have full access to the interconnect bandwidth, not just the master switch. The master switch is elected from one of the stack members. It automatically configures the stack with the currently running IOS image and a single configuration file.

The switches are connected with special cables that form a bidirectional closed loop path.

The stack has a single management IP address and is managed as a unit.

Up to nine switches can be in a stack.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Describe the benefits of switch stacking and chassis aggregation



References:

[Products & Services > Switches > Campus LAN Switches - Access > Cisco Catalyst 3750 Series Switches > Data Sheets and Literature > White Papers > Cisco StackWise and StackWise Plus Technology](#)

QUESTION 14

RouterA and RouterB, which connect two locations, are unable to communicate. You run the show running-configuration command on both router interfaces, RouterA and RouterB. The following is a partial output:

```
routerA#show running-config
interface Serial0
description Router_A
ip address 192.10.191.2 255.255.255.0
encapsulation ppp
no ip mroute-cache
clockrate 64000
```

```
routerB#show running-config
interface Serial1
description Router_B
ip address 192.10.192.1 255.255.255.0
encapsulation ppp
no ip mroute-cache
clockrate 64000
```

Based on the information given in the output, what are two likely causes of the problem? (Choose two.)

- A. The IP address defined is incorrect.
- B. Both routers cannot have a clock rate defined.
- C. Both routers cannot have an identical clock rate.
- D. The Layer 2 framing is misconfigured.
- E. At least one of the routers must have the ip mroute-cache command enabled.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Two possible causes of the problem are that the IP addresses are incorrect as defined, or that both routers have a defined clock rate. The IP addresses on the routers are in different subnets. The IP addresses need to be changed to fall in the same subnet.

Both routers cannot have a clock rate configured. Only routers with a DCE cable connected should have a clock rate, which provides synchronization to the router connected to the DTE cable. In a point-to-point serial connection, the DCE cable connects to the DTE cable, providing a communication path between the two routers. If both computers have a clock rate configured, the routers will not communicate.

A matching clock rate is not the problem. The clock rates between two routers should match. The router connected to the DCE cable will provide the clock rate to the router connected to the DTE cable, resulting in matching clock rates.

The Layer 2 encapsulation refers to the Data Link protocol used on the link. In this case, the protocol is Point to Point Protocol (PPP), which is configured correctly on both ends as indicated by the matching encapsulation ppp statements in the output. The connection would be prevented from working if one of the routers were missing this setting (which would be indicated by the absence of the encapsulation ppp statement in its output), or if a different Layer 2 encapsulation type were configured, such as High-Level Data Link Control (HDLC).

The ip mroute-cache command is used to fast-switch multicast packets and would not cause the problem in this scenario.

Objective:

Network Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

[Cisco > Internetworking Technology Handbook > Point to Point Protocol \(PPP\)](#)

[Cisco > Support > Product Support > Cisco IOS Software Releases 11.1 > Configure > Feature Guides > Clock Rate Command Enhancements Feature Module > clock rate](#)

QUESTION 15

Which of the following commands will set the line speed of a serial connection that connects to a Channel Service Unit /Digital Service Unit (CSU/DSU) at 56 Kbps?

- A. service-module 56000 clock rate speed
- B. service-module 56k clock rate speed
- C. bandwidth 56k
- D. bandwidth 56000

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The command `service-module 56k clock rate speed` will configure the network line speed for a 4-wire, 56/64-kbps CSU/DSU module.

The command `service-module 56000 clock rate speed` is incorrect because the speed must be stated in the form 56k (for Kbps), rather than 56000.

The `bandwidth` command is used to limit the amount of bandwidth used by an application when utilizing Quality of Service (QoS). It does not set the line speed of a serial connection that connects to a Channel Service Unit /Digital Service Unit CSU/DSU. Therefore, both the `bandwidth 56k` and the `bandwidth 56000` commands are incorrect.

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

References:

[Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.4T > Part 2: Serial Interfaces > Configuring Serial Interfaces > 2-Wire and 4-Wire, 56/64-kbps CSU/DSU Service Module Configuration Task List > Setting the Network Line Speed](#)

QUESTION 16

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 IPv4 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 17

Which of the following techniques is NOT used by distance vector protocols to stop routing loops in a network?

- A. Split horizon
- B. Spanning Tree Protocol (STP)
- C. Holddowns
- D. Route poisoning

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Spanning Tree Protocol (STP) is not used by distance vector protocols to stop routing loops in a network. STP is used to prevent switching loops in a switched network.

Routing loops can occur due to slow convergence and inconsistent routing tables, and can cause excessive use of bandwidth or complete network failure. An example of a routing table problem would be incorrectly configured static default routes. Suppose that Router A is connected to Router B, and the addresses of the interfaces on each end of the link connecting the two routers are as follows:

Router A 192.168.5.1/24

Router B 192.168.5.2/24

A partial output of the routing tables of the two routers is shown below. Router B hosts the connection to the Internet.

```
routerA# show ip route
Gateway of last resort is 192.168.5.2 to network 0.0.0.0
<Output omitted>
```

```
routerB# show ip route
Gateway of last resort is 192.168.5.1 to network 0.0.0.0
<<output omitted>>
```

From the limited information shown above, you can see that Router A is pointing to Router B for the default route, and Router B is pointing to Router A for the default route. This will cause a routing loop for any traffic that is not in their routing tables. For example, if a ping were initiated to the address 103.5.6.8 and that address was not in the routing tables of Routers A and B, the most likely message received back would NOT be "destination unreachable" but "TTL expired in transit." This would be caused by the packet looping between the two routers until the TTL expired.

The following techniques are used by distance vector protocols to stop routing loops in a network:

- Split horizon stops routing loops by preventing route update information from being sent back over the same interface on which it arrived.
- Holddown timers prevent regular update messages from reinstating a route that is unstable. The holddown timer places the route in a suspended, or "possibly down" state in the routing table and regular update messages regarding this route will be ignored until the timer expires.
- Route poisoning "poisons" a failed route by increasing its cost to infinity (16 hops, if using RIP). Route poisoning is combined with triggered updates to ensure fast convergence in the event of a network change.

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 18

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 19

When packets are transmitted from one host to another across a routed segment, which two addresses are changed? (Choose two.)

- A. source IP address
- B. source MAC address
- C. destination IP address
- D. destination MAC address

Correct Answer: BD

Section: (none)

Explanation

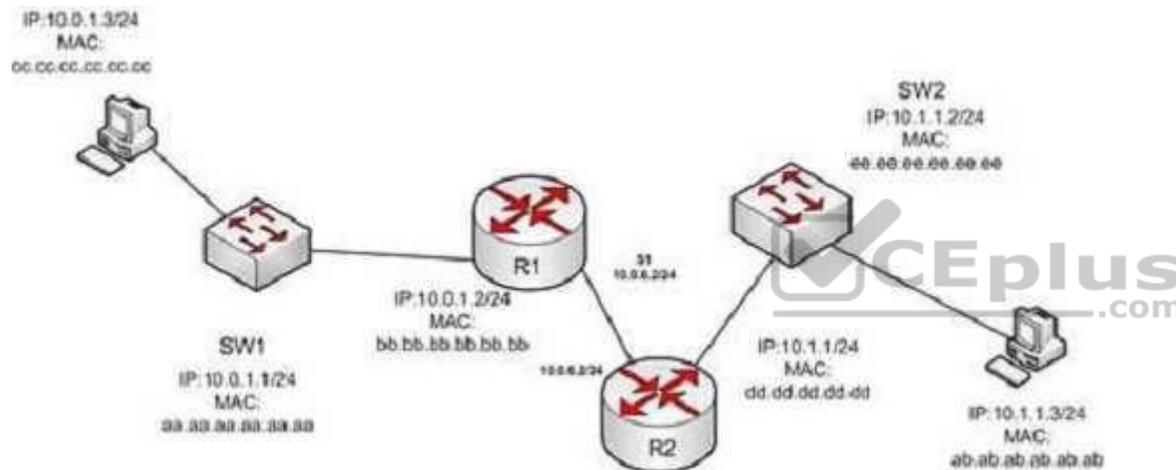
Explanation/Reference:

Explanation:

When packets move from one LAN segment to another LAN segment across a router, the source and destination Media Access Control (MAC) addresses in the packet change.

Packets destined for a remote network must be forwarded by a router that is typically the sending host's default gateway. The IP address of the remote host is inserted into the packet, while the MAC address of the default gateway is inserted as the Layer 2 address. This ensures that the packet is received by the default gateway. The router then examines the destination IP address, performs a route lookup, and forwards the packet toward the destination, inserting its MAC address as the source MAC address. If the next hop is another router, then the destination MAC address is replaced with the next router's MAC address. This process is repeated by each router along the path (inserting its own MAC address as the source MAC address and inserting the MAC address of the next router interface as the destination MAC address) until the packet is received by the remote host's default gateway. The destination gateway then replaces the destination MAC address with the host's MAC address and forwards the packet.

In the diagram below, when the host located at the IP address 10.0.1.3 sends data to the host located at IP address 10.1.1.3, the Layer 2 and Layer 3 destination addresses will be bb.bb.bb.bb.bb.bb and 10.1.1.3, respectively. Note that the Layer 2 destination address matches the host's default gateway and not the address of the switch or the destination host.



It is incorrect to state that the source IP address or the destination IP address change when packets transfer from one host to another across a routed segment. The Internet Protocol (IP) addresses within the packets do not change because this information is needed to route the packet, including any data returned to the sender.

Data return to the sending host is critically dependent on the destination having a default gateway configured and its router having a route back to the sender. If either is missing or configured incorrectly, a return is not possible. For example, when managing a switch remotely with Telnet, the switch cannot be located on the other side of a router from the host being used to connect if the switch does not have a gateway configured. In this case, there will no possibility of a connection being made because the switch will not have a return path to the router.

Objective:
 Routing Fundamentals Sub-
 Objective:

Describe the routing concepts

References:

[Cisco Documentation > Internetworking Technology Handbook > Routing Basics](#)

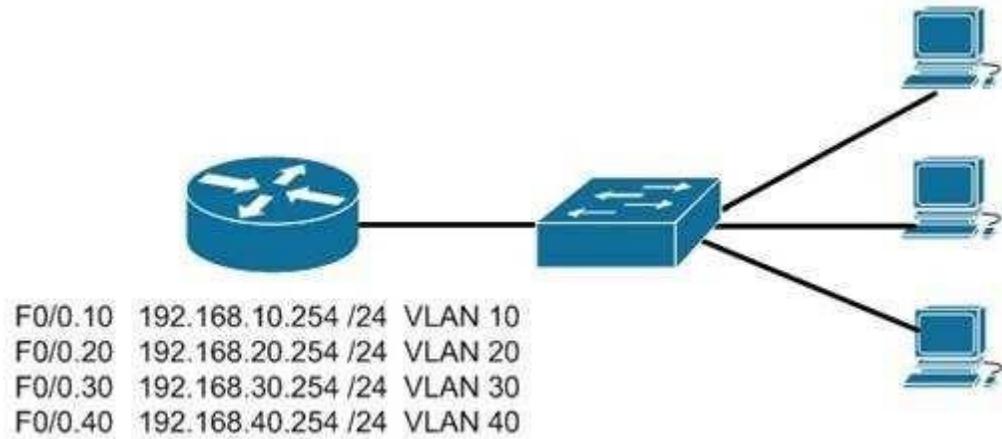
QUESTION 20

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 21

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

- C.
- A. CSU/DSU
- B. switch
- 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 22

You are a network administrator for your organization. Your organization has two Virtual LANs, named Marketing and Production. All Cisco 2950 switches in the network have both VLANs configured on them. Switches A, C, F, and G have user machines connected for both VLANs, whereas switches B, D, and E have user machines connected for the Production VLAN only. (Click the Exhibit(s) button to view the network diagram.)

You receive a request to configure Fast Ethernet port 0/2 on Switch B for a user computer in the Marketing VLAN. VLAN numbers for the Marketing and Production VLANs are 15 and 20, respectively.

Which Cisco 2950 switch command should you use to configure the port?

C.



<https://vceplus.com/>

- A. SwitchB(config-if)#switchport trunk vlan 15
- B. SwitchB(config)#switchport access vlan 15
- SwitchB(config-if)#switchport access vlan 15
- D. SwitchB(config-if)#switchport trunk vlan 15, 20

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The SwitchB(config-if)#switchport access vlan 15 command should be used to enable the port for the Marketing VLAN in access link mode. You must first enter the interface configuration mode by using the following command:

```
SwitchB(config)#interface fast 0/2
```

When executing the command switchport access vlan vlan #, if the VLAN number does NOT match that of the correct VLAN, the host connected to this port will not be in the correct VLAN. If the VLAN number doesn't exist, the host will not be able to communicate with any resources on the LAN.

User machines are always connected to an access link. A trunk link is used to span multiple VLANs from one switch to another or from a switch to a router. For inter- VLAN routing to function, the port that is connected to the router must be configured as a trunk port. To configure a port into trunk mode, you should use the following command:

```
SwitchB(config-if)#switchport mode trunk
```



C.

The SwitchB(config)#switchport access vlan 15 command is incorrect because the router is in global configuration mode. The switchport command is applied in the interface configuration mode.

All other options are incorrect because the access parameter should be used with the switchport command. The trunk parameter is used to add allowed VLANs on the trunk. The correct command syntax is:

```
switchport trunk {{allowed vlan vlan-list} | {native vlan vlan-id} | {pruning vlan vlan-list}}
```

Objective:

LAN Switching Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

QUESTION 23

You are configuring a PPP connection between two routers, R1 and R2. The password for the connection will be poppycock. When you are finished you execute the show run command on R1 to verify the configuration.



Which of the following examples of partial output of the show run command from R1 represents a correct configuration of PPP on R1?

- A. enable password griswald hostname
R1 username R1 password poppycock
interface serial 0/0 ip address
192.168.5.5 255.255.255.0
encapsulation ppp ppp
authentication chap
- B. enable password griswald hostname
R1 username R1 password poppycok
interface serial 0/1 ip address
192.168.5.5 255.255.255.0
encapsulation ppp ppp
authentication chap
- C. enable password griswald hostname
R1 username R2 password poppycock
interface serial 0/0 ip address
192.168.5.5 255.255.255.0
encapsulation ppp ppp
authentication chap
- D. enable password griswald hostname
R1 username R1 password griswald
interface serial 0/0 ip address
192.168.5.5 255.255.255.0
encapsulation ppp ppp
authentication chap



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The correct configuration is as follows:

```
enable password griswald  
hostname R1 username R2
```

```
password poppycock interface
serial 0/0
ip address 192.168.5.5 255.255.255.0
encapsulation ppp ppp authentication
chap
```

The key settings that are common problems are as follows:

- The username is set to the hostname of the other router (in this case, R2) ▪
The password is set poppycock which must be the same in both routers

The following set is incorrect because the username is set to the local hostname (R1) and not the hostname of the other router (R2):

```
enable password griswald hostname R1
username R1 password poppycock
interface serial 0/0 ip address
192.168.5.5 255.255.255.0
encapsulation ppp ppp authentication
chap
```

The following set is incorrect because the password is misspelled. It should be poppycock, not poppycok.

```
enable password griswald hostname R1
username R1 password poppycok
interface serial 0/0 ip address
192.168.5.5 255.255.255.0
encapsulation ppp ppp authentication
chap
```

The following set is incorrect because the password is set to the enable password of the local router (R1) rather than the agreed upon PPP password, which is poppycock.

```
enable password griswald hostname R1
username R1 password griswald
interface serial 0/0 ip address
192.168.5.5 255.255.255.0
encapsulation ppp ppp authentication
chap
```

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 24

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-

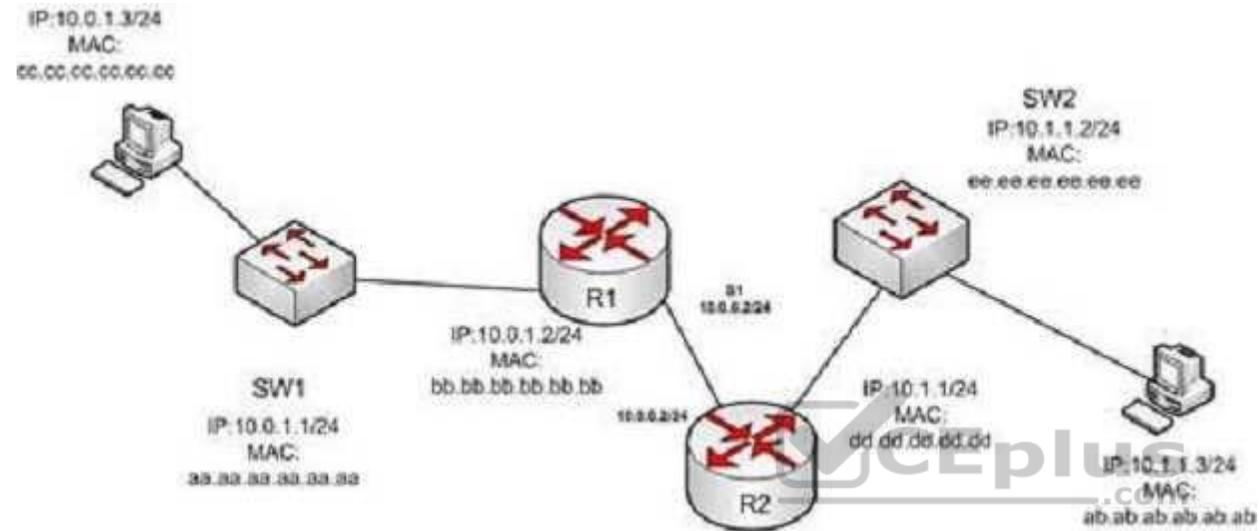
Objective:

Compare and contrast TCP and UDP protocols

References:

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.dd
- D. cc.cc.cc.cc.cc.cc
- E. aa.aa.aa.aa.aa.aa
- F. bb.bb.bb.bb.bb.bb

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The source physical address of the packet when it 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

What command was used to generate the output shown below?

```
Connection-specific DNS Suffix . : ajax.acme.com
Description . . . . . : Broadcom NetXtreme 57xx Gigabit Controller

Physical Address. . . . . : 00-1A-A0-E1-95-AB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ada3:8b73:a66e:6bc0%10 (Preferred)
IPv4 Address. . . . . : 10.88.2.177 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, October 05, 2011 4:31:32 PM
Lease Expires . . . . . : Friday, October 07, 2011 4:33:32 AM
Default Gateway . . . . . : 10.88.2.6
DHCP Server . . . . . : 10.88.10.48
DHCPv6 IAID . . . . . : 234887840
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-EE-0F-98-00-1A-A0-E1-95-AB

DNS Servers . . . . . : 10.88.10.48
10.75.139.18
NetBIOS over Tcpiip. . . . . : Enabled
```

- A. winipcfg
- B. ipconfig
- C. ifconfig

D. ipconfig/all

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The output displayed is that generated by the ipconfig/all command as executed on a Windows computer. This command displays a wealth of information about the current configuration. Examples of information that can be gleaned from the sample output include:

- The router for computer is at 10.88.2.6.
- The primary DNS server is 10.88.10.49.
- The address of the computer is 10.88.2.177. Any packets that need to be sent to any computers in the 10.88.2.0/24 network will not use the default gateway but will be switched to the destination by MAC address. Packets that need to be sent to any other network, however, will require the use of the default gateway and so the frame will be switched to MAC address of the gateway.

This information can be used with other utilities for troubleshooting. For example, if you can ping the primary DNS server at 10.88.10.49, which in a remote network, then the IP address is correct and your router (10.88.2.6) knows a route to the network where the DNS server is located. However, this result would NOT prove that DNS is working correctly. Verification would require successfully pinging local or remote hosts by name rather than IP address.

It is not the output of winipcfg. This command was used in Windows 95 to generate a subset of this information in a GUI dialog box.

It is not the output of ifconfig. This command is used to generate a subset of this information in a Linux/Unix environment.

It is not the output of ipconfig. This command generates IP address subnet mask and gateway only.

Objective:

Network Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

[Cisco>Home>Support>Technology Support>IP>IP Addressing Services>Configure>Configuration Examples and TechNotes> Dynamically Configuring DHCP Server Options>Troubleshoot](#)

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:

QUESTION 30

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

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

Telnet does not use IMAP. Telnet is an application that remotely accesses a computer for the purpose of executing commands. It uses TCP port 23 to connect to the remote computer.

Objective:

Network Fundamentals Sub-

Objective:

Compare and contrast TCP and UDP protocols

References:

[Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems>OSI Model Application Layer](#)

QUESTION 31

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 32

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 33

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 34

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 0
FastEthernet0/1 0 0 0 0 0 0 0 0 0
Serial0/1 0 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 35

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 36

A host is powered up, but the connected switch port does not turn amber or green.

Which of the following methods would you use to troubleshoot the situation? (Choose three. Each answer is a complete solution.)

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

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

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

Objective:

LAN Switching Fundamentals Sub-

Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

[Cisco > Catalyst 2960 Switch Hardware Installation Guide > LEDs](#)

QUESTION 37

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)

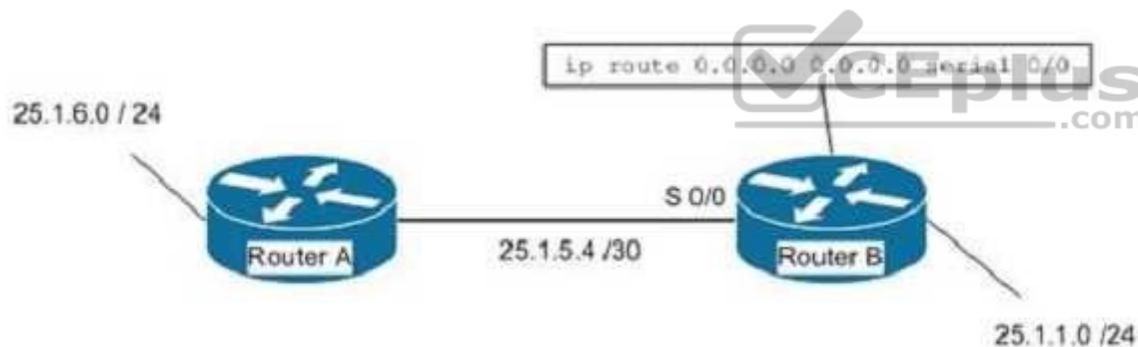
Explanation

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 38

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 encapsulation type that supports both synchronous and asynchronous circuits and provides built-in security mechanisms. 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 absence 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
<output omitted>
interface serial 0/0
encapsulation ppp

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

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 39

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 40

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. 255.255.255.192
- C. 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 = $2^{\text{number-of-subnet-bits}}$

Number of hosts per subnet = $2^{\text{number-of-host-bits}} - 2$

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: $2^8 = 256$

Hosts that can be used: $2^8 - 2 = 254$

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 ($2^{14} - 2 = 16382$). However, there will be 4 subnets ($2^2 = 4$).

If you use 255.255.255.192 as the subnet mask, there will be 62 hosts ($2^6 - 2 = 62$).

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

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 ($2^{\text{number-of-host-bits}} - 2$) 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 ($2^{\text{number-of-subnet-bits}}$) 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 ($2^{\text{number-of-subnet-bits}} - 2$) 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 41

When the copy running-config startup-config command is issued on a router, where is the configuration saved?

- A. Random access memory (RAM)
- B. Flash
- C. Non-volatile random access memory (NVRAM)
- D. Read-only memory (ROM)

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When the copy running-config startup-config command is issued on a router, the configuration is saved in the non-volatile random access memory (NVRAM) memory. The copy startup-config running-config command copies the version in RAM to NVRAM.

Note: For the copy startup-config running-config command to function, there must be a configuration already residing in RAM. For example, a brand-new router with no configuration created would have no startup configuration in RAM. If you attempted to execute the copy startup-config running-config command in that case, you would receive the following error message

```
%% non-volatile memory configuration is invalid or not present
```

In addition to storing the running configuration in the NVRAM, you can also store it on a Trivial File Transfer Protocol (TFTP) server. When a router boots in the absence of a startup configuration, the router will look for a valid configuration on a TFTP server. In the case that the TFTP server also does not have a valid router configuration or is unreachable, the router will enter the setup dialog and prompt the user to provide initial configuration inputs.

The router does not store the startup configuration in random access memory (RAM). RAM only holds the running configuration that is loaded from the NVRAM or TFTP server during the boot process.

The router does not store the configuration in flash or read-only memory (ROM). ROM contains the bootstrap code, while flash memory contains the IOS image.

Objective:

Infrastructure Management Sub-

Objective:

Perform device maintenance

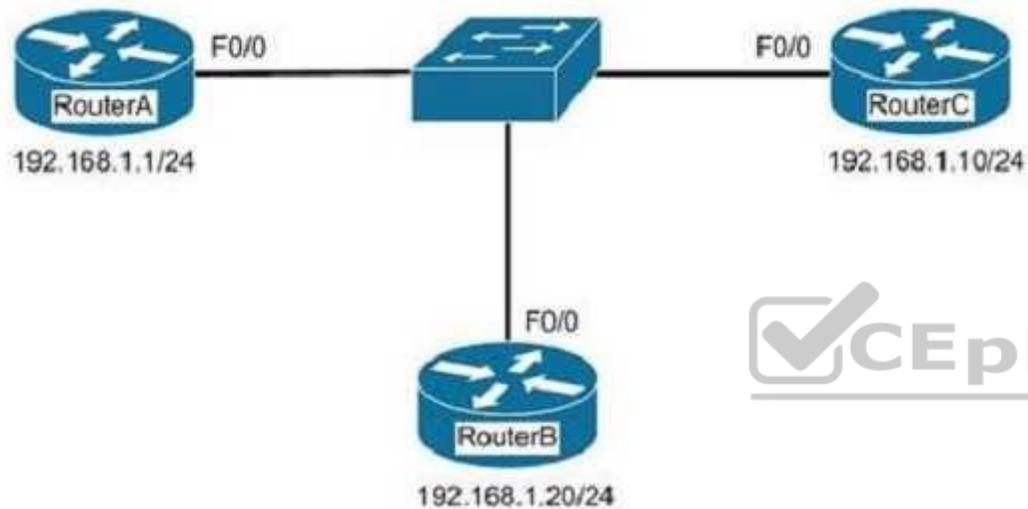
References:

[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 42

In the network exhibit, the routers are running OSPF and are set to the default configurations. (Click the Exhibit(s) button.)



What would be the effect of configuring a loopback interface on RouterA with an address of 192.168.1.50/24?

- A. Router B would become the DR
- B. Router A would become the DR
- C. Router C would become the DR
- D. Router A would become the BDR

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Configuring a loopback interface on RouterA with an address of 192.168.1.50/24 would cause Router A to become the designated router (DR). The designated router (DR) is determined by the router with the highest interface priority number. If the priority numbers are tied, then the router with the highest router ID (RID) becomes the DR.

The default priority number is 1, and can be configured as high as 255. Changing the priority to 0 would make the router ineligible to become the DR or the backup designated router (BDR). The `ip ospf priority #` command is used to manually configure a priority on a specific interface.

Router IDs are determined first by the highest loopback IP address, followed by the highest IP address on an active physical interface. Thus, in the case of a priority tie, the router with the highest loopback IP address will have the highest RID, and will become the DR for the network segment.

The current Router ID for a router can be determined by executing the `show ip interface brief` command. In the sample output of the `show ip interface brief` command below, the RID will be 10.108.200.5.

```
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
```



Neither Router B nor C will be the DR because the IP addresses on their physical interfaces are lower than 192.168.1.50/24.

Router A will not be the backup designated router. Since it is the DR, it cannot also be the BDR.

Router C will not be the BDR because its IP address is lower than that of Router B. Router B will be the BDR.

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 43

Which command produced the following output?

```
<output omitted>
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 msec
Retransmission pacing timer 110 msec
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
```



- 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 output was produced by the show ip ospf command. The show ip ospf command is used to view information about the OSPF routing processes. 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 show ip ospf database command is incorrect because this command is used to view the OSPF database for a specific router. The following is sample output from the show ip ospf database command when no arguments or keywords are used:

```
Router# show ip ospf database
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Router Link States(Area 0.0.0.0)
Link ID ADV Router Age Seq# Checksum Link count
172.16.21.6 172.16.21.6 1724 0x80002CFB 0x69BC 5
172.16.21.5 172.16.21.5 2512 0x800009D2 0xA2B8 3
172.16.1.2 172.16.1.2 1659 0x80000A98 0x4CB6 7
172.16.1.1 172.16.1.1 5115 0x800009B6 0x5F2C 9
172.16.1.5 172.16.1.5 1626 0x80002BC 0x2A1A 4
172.16.65.6 172.16.65.6 1315 0x80001947 0xEEE1 9
172.16.241.5 172.16.241.5 1123 0x8000007C 0x7C70 1
172.16.27.6 172.16.27.6 1712 0x80000548 0xB641 4
172.16.70.6 172.16.70.6 1142 0x80000B97 0xEB84 6
Displaying Net Link States(Area 0.0.0.0)
Link ID ADV Router Age Seq# Checksum
172.16.1.3 192.168.239.66 1245 0x800000EC 0x82E
Displaying Summary Net Link States(Area 0.0.0.0)
Link ID ADV Router Age Seq# Checksum
172.16.240.0 172.16.241.5 1152 0x80000077 0x7A05
172.16.241.0 172.16.241.5 1152 0x80000070 0xAEB7
172.16.244.0 172.16.241.5 1152 0x80000071 0x95CB
```

The show ip ospf statistics command is incorrect because this command is used to view the OSPF calculation statistics. The following is sample output from the show ip ospf statistics command that shows a single line of information for each SPF calculation:

```
Router# show ip ospf statistics
OSPF process ID 200
-----
Area 0: SPF algorithm executed 10 times
Area 200: SPF algorithm executed 8 times
Summary OSPF SPF statistic
SPF calculation time
Delta T Intra D-Intra Summ D-Summ Ext D-Ext Total Reason
08:17:16 0 0 0 0 0 0 0 R,
08:16:47 0 0 0 0 0 0 0 R, N,
08:16:37 0 0 0 0 0 0 0 R, X
00:04:40 208 40 208 44 220 0 720 R, N, SN, X
00:03:15 0 112 4 108 8 96 328 R, N, SN, X
00:02:55 164 40 176 44 188 0 612 R, N, SN, X
00:01:49 0 4 4 0 4 4 16 R, N, SN, X
00:01:48 0 0 4 0 4 0 12 R, N, SN, SA, X
00:01:43 0 0 4 0 4 0 8 R,
00:00:53 164 40 176 44 188 0 612 R, N, SN, X
```



The show ip ospf traffic command is incorrect because this is not a valid command.

Objective:

Routing Fundamentals Sub-

Objective:

Compare and contrast interior and exterior routing protocols

References:

[Cisco > Cisco IOS IP Routing Protocols Command Reference > OSPF Commands: show ip ospf through T > show ip ospf](#)

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 9: OSPF, p. 375.

QUESTION 44

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 45

You are the Cisco administrator for NationalAct Incorporated. One of your assistants is preparing to introduce a new switch to the network. Before doing so, you execute the show vtp status command on OldSwitch and NewSwitch, respectively, and receive the following output:

```
OldSwitch# 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
<output omitted>
```

```
NewSwitch# show vtp status
VTP Version : 2
Configuration Revision : 125
Maximum VLANs supported locally : 1005
Number of existing VLANs : 10
VTP Operating Mode : Server
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
<output omitted>
```



If NewSwitch is introduced to the network, which of the following will be true?

- A. NewSwitch will delete its current VTP data.
- B. There will be 10 VLANs in the network.
- C. OldSwitch will retain its current VTP data.
- D. There will be 24 VLANs in the network.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If NewSwitch is introduced to the network, there will be 10 VLANs. 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.

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 Configuration Revision: 125 output indicates that NewSwitch has a configuration revision number of 125, which will be compared to other switches in the same VTP domain, including OldSwitch, which has a revision number of 62. If the production switches have lower configuration revision numbers than the new switch, their VLAN databases will be replaced with the VLAN database of the new switch. Any switch ports that had been assigned to be removed from VLANs in the configuration database of the new switch 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.

NewSwitch will not delete its current VTP data. If the production switches have lower configuration revision numbers than the new switch, their VLAN databases will be replaced with the VLAN database of the new switch.

The number of VLANs will not remain 24. The 24 VLANs indicated by the Number of existing VLANs: 24 output will be overwritten with the 10 VLANs in the NewSwitch VLAN database.

OldSwitch will not retain its current VTP data. It will be replaced with the VLAN database of the new switch.

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](#) CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 1: Virtual LAN Concepts, pp. 16-20. CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 1: Virtual LAN Concepts, pp. 38-42.

QUESTION 46

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 47

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.

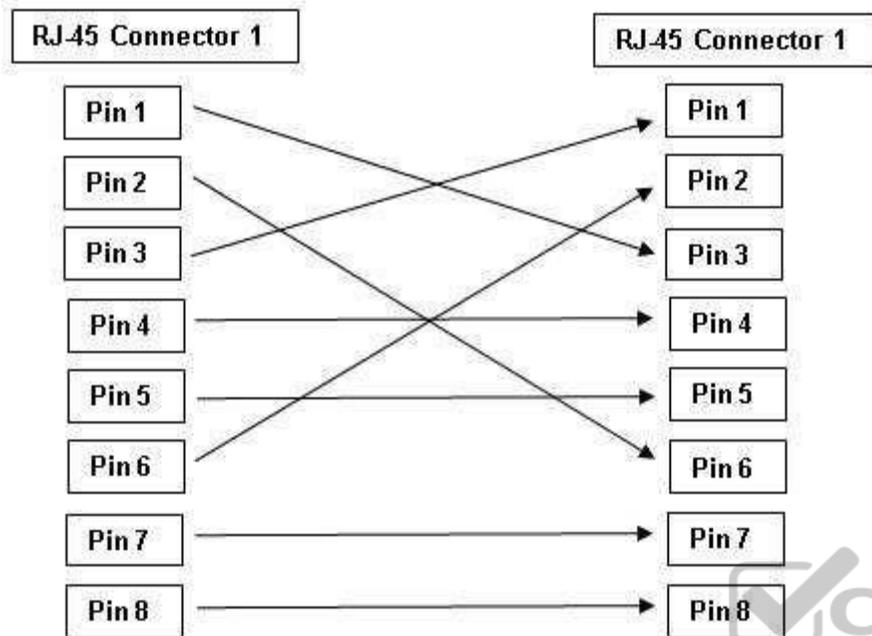
A crossover cable is used to connect "like" devices, and a straight through cable is used when connecting "unlike" devices. The one exception to this rule is when connecting a computer NIC to an Ethernet port on a router, a crossover cable is used. In summary, the following list describes when to use 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 48

What command would you run to determine which switch is the root bridge for a particular VLAN?

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

- D. show spanning-tree vlan
- E. show spanning-tree interface

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show spanning-tree vlan command provides Spanning Tree Protocol (STP) information on the root switch, including the bridge ID, root path, and root cost, as well as information on the local switch. The output of the command is as follows:

```
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

Interface      Role      Sts      Cost      Prio.Nbr      Type
-----
Fa0/2          Root      FWD      19         128.2         P2p
Fa0/10         Desg     FWD      19         128.10        P2p
Fa0/1          Altn     BLK      19         128.1         P2p
```

This output indicates the following:

- The root switch has a bridge ID (Priority + MAC Address) of 0-000c.00d3.5124, while the local switch has a bridge ID of 32769-000c.14f5.b5c0. This indicates that the local switch is not the root switch for VLAN 1. Additional evidence that the local switch is not the root switch is the fact that the Fa0/1 port is blocking with a role listed as Altn. Only non- root bridges have blocking ports.

- For this switch, Fa0/1 represents the redundant link that needs to be blocked to prevent a switching loop.
- Interface Fa0/2 is the root port (the interface with the shortest path to the root switch).
- All three links have a cost of 19, which is the default cost of a single FastEthernet link.
- 802.1d is enabled in this switch, as indicated by the output Spanning tree enabled protocol ieee in line 2.

The show spanning-tree interface command will indicate the port role and state that a particular interface plays in each VLAN, but does not indicate the root bridge for a particular VLAN. Below is sample output from the show spanning-tree interface fastethernet0/1 command. In this example, RSTP is in use rather than 802.1d.

```
Switch# show spanning-tree interface fastethernet0/1
```

VLAN	Role	Sts	Cost	Prior.Nbr	Type
VLAN0001	Altn	BLK	19	128.2	P2P
VLAN0002	Root	FWD	19	128.1	P2P
VLAN0003	Root	FWD	19	128.1	P2P

In the above output, the Fa0/1 interface is not the root bridge for any of the three VLANs. It is the root port for VLANs 2 and 3. Root bridges have only designated ports. It is the alternate port for VLAN1, which means that Fa0/1 has a higher cost path to the root bridge than another interface in the topology, and will be in a blocking state as long as that other path is available.

The other options are incorrect because they are not valid Cisco IOS commands. The correct syntax would be show spanning-tree, not show spanning tree or show spantree.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot STP protocols

References:

[Cisco > Cisco IOS Switching Command Reference > show spanning-tree](#)

QUESTION 49

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 50

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
255.255.255.0 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 51

```
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 52

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 53

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 54

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 55

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

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

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

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

```
Router78# show version
Cisco IOS Software, 3800 Software (C3845-IPBASE-M), Version 12.3(11)T7, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sat 30-Jul-05 03:12 by dchih

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

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

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

Configuration register is 0x2102
```

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

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

Objective:

LAN Switching Fundamentals Sub-

Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

QUESTION 56

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 57

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, NVRAM
- E. 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 58

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



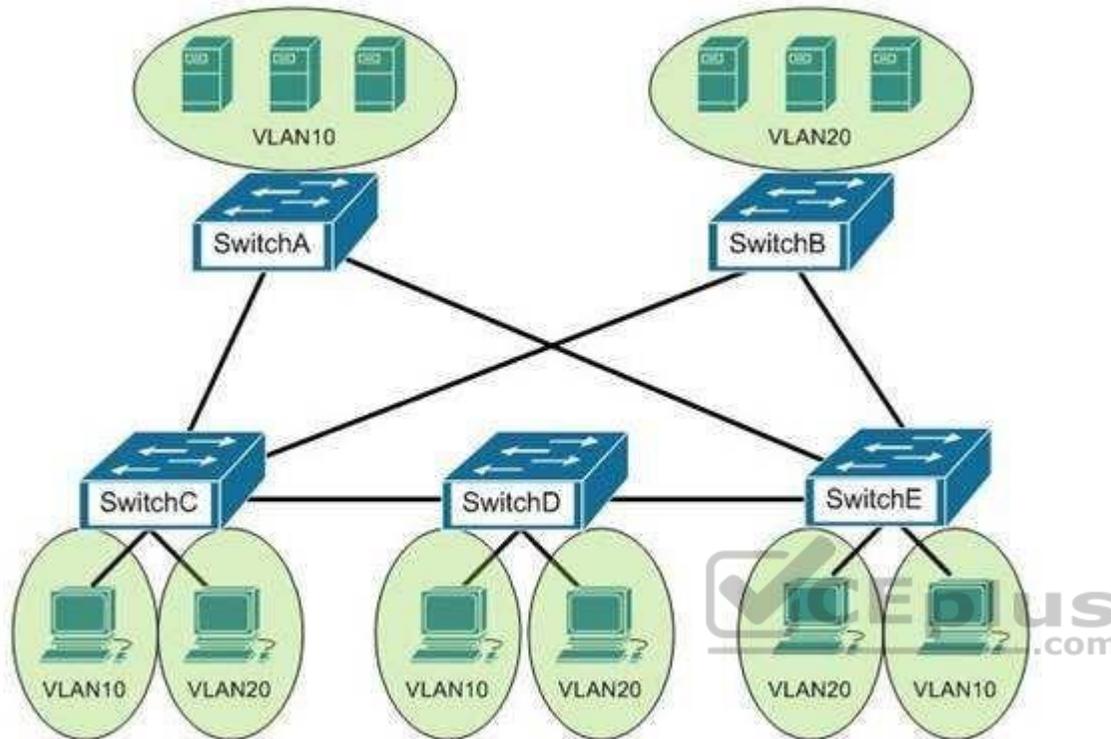
References:

[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 59

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:

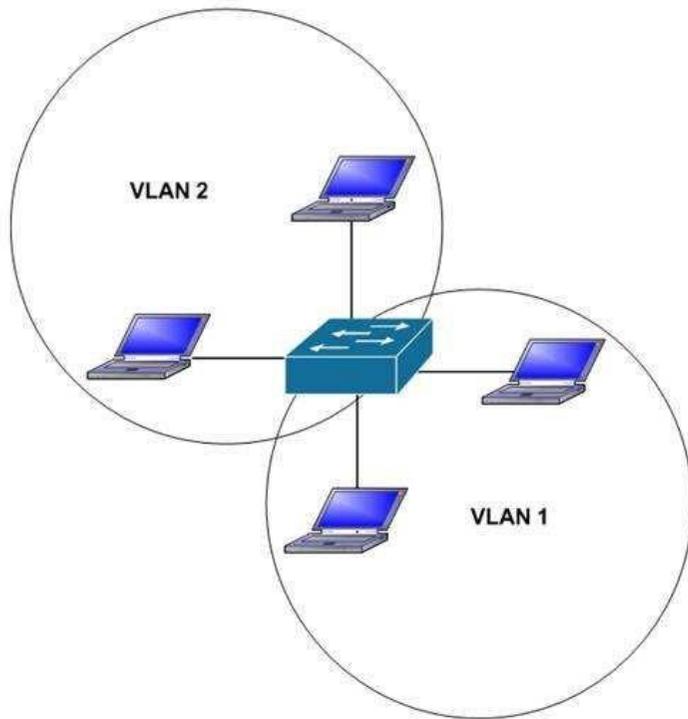
Configure, verify, and troubleshoot STP protocols

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 60

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 61

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 62

What is the purpose of frame tagging in Virtual LAN (VLAN) configurations?

- A. inter-VLAN routing
- B. encryption of network packets
- C. frame identification over trunk links
- D. frame identification over access links

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Frame tagging is used when VLAN traffic travels over a trunk link. Trunk links carry frames for multiple VLANs. Therefore, frame tags are used for identification of frames from different VLANs. Inter Switch Link (ISL) and Institute of Electrical and Electronics Engineers (IEEE) 802.1q are the two frame tagging methods supported on Cisco devices.

The purpose of frame tagging is not inter-VLAN routing. A Layer 3 device, such as a router or multilayer switch, is used for inter-VLAN routing. To configure interVLAN routing a logical or subinterface for each VLAN must be created on the single physical interface used to connect to the switch. An IP address is NOT applied to the physical interface; instead, each subinterface is configured with an IP address that will become the default gateway of all devices residing in that VLAN. Consequently, each subinterface and its VLAN devices must reside a different subnet as well. If a subinterface on the router is NOT configured with an IP address that resides in the same network as the hosts that reside in the VLAN that the subinterface serves, the hosts in that VLAN will be isolated from the other VLANs. The hosts in the VLAN served by the subinterface should also use this address as their default gateway, or the hosts in the VLAN will likewise be isolated from the other VLANs

To verify the IP address of the subinterface, execute the show interfaces subinterface ID command. As shown below, the IP address will appear in line 3 of the output. Compare this IP address will the IP address set as the default gateway of each host in the VLAN served by the subinterface. They should be the same, and the IP address of the hosts should be in the same subnet as this address as well.

```
router# show interfaces fastEthernet 0/0.1
FastEthernet0/0.1 is up, line protocol is up
Hardware is AmdFE, address is 0003.e36f.41e0 (bia 0003.e36f.41e0)
Internet address is 10.10.10.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ISL Virtual LAN, Color 1.
ARP type: ARPA, ARP Timeout 04:00:00
```

Frame tagging does not provide encryption of network packets. Packets are transmitted unencrypted unless the network device or the application uses an additional encryption mechanism. A Virtual Private Network (VPN) is a popular solution for providing encrypted network communication.

An access link is a connection between a switch and an end-user computer with a normal Ethernet Network Interface Card (NIC). On these links, Ethernet frames are transmitted without frame tagging.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

[Cisco > Cisco IOS LAN Switching Configuration Guide, Release 12.4 > Part 1: Virtual LANs > Routing Between VLANs Overview](#)

[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 63

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 64

Which set of Cisco Internetwork Operating System (IOS) commands is used on Cisco routers to set a password for Telnet lines?

- A.

```
router(config-router)# line vty 0
4router(config-line)# login
router(config-line)# password password
```
- B.

```
router(config)# line telnet 0 4router(config-
line)# login
router(config-line)# password password
```
- C.

```
router(config)# line aux 0router(config-line)#
login
router(config-line)# password password
```
- D.

```
router(config)# line vty 0 4router(config-line)#
login router(config-line)# password password
```

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The following commands are used on Cisco routers to set a password for Telnet lines:

```
router(config)# line vty 0 4 router(config-  
line)# login router(config-line)# password  
password
```

An explanation of the commands is below:

router(config)# line vty 0 4: Enters line configuration mode for virtual terminal lines 0 to 4. router(config-line)# login: Ensures that any remote access is prompted for a password. router(config-line)# password password: Sets a password of "password" for VTY lines.

Assigning a password to the VTY lines is required for remote connections to the device to be possible. If a password has not been configured the following error message will be generated when the connection is attempted:

```
Password required but not set
```

```
[Connection to foreign host 106.5.5.1 closed by foreign host]
```

Configuring a VTY password and requiring the password (accomplished with the login command) is good first step in securing Telnet access to the device. Another step that can enhance the security of remote access to the device would be to apply an access list to the VTY lines with the access-class command.

The command sequence which begins with router(config-router)# line vty 0 4 is incorrect because the line vty 0 4 command should be executed in global configuration mode, not routing protocol configuration mode.

The line telnet 0 4 command is incorrect because this is not a valid Cisco IOS command.

The line aux 0 command is incorrect because this allows you to configure the properties of the Auxiliary port, as opposed to the incoming Telnet (VTY) lines.

Objective:

Infrastructure Management Sub-

Objective:

Configure and verify device management

References:

[Cisco > Support > Technology Support > IP > IP Addressing Services > Design > Design TechNotes > Cisco Guide to Harden Cisco IOS Devices > Document ID: 13608](#)

[Cisco > Support > End-of-sale and End-of-life Products > Cisco IOS Software Releases 11.0 > Configuration Examples and TechNotes > Telnet, Console and AUX Port Passwords on Cisco Routers Configuration Example](#)

QUESTION 65

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 66

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-and-play 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](#)

QUESTION 67

Which of the following is NOT a feature offered by Enhanced Interior Gateway Routing Protocol (EIGRP)?

- A. variable length subnet masks (VLSM)
- B. partial updates
- C. neighbor discovery mechanism
- D. multiple vendor compatibility

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EIGRP is a Cisco-proprietary routing protocol, and does not support multiple vendor environments.

EIGRP is a classless routing protocol, and thus supports variable length subnet masks (VLSM).

EIGRP routers build a neighbor table in memory, and use a multicast-based neighbor discovery mechanism.

EIGRP routers send partial updates when there are network events.

The following are features offered by EIGRP:

- Fast convergence
- Partial updates
- Neighbor discovery mechanism
- VLSM
- Route summarization
- Scalability

Objective: Routing

Fundamentals Sub-

Objective:

Compare and contrast distance vector and link-state routing protocols

References:

[Cisco > Support > IP > IP Routing > Design > Design TechNotes > Introduction to EIGRP > Document ID: 13669](#)

QUESTION 68

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 69

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 70

Which two statements are TRUE of Internet Protocol (IP) addressing? (Choose two.)

- A. Public addresses are registered with the Internet Assigned Numbers Authority (IANA).
- B. These addresses are publicly registered with the Internet Service Provider (ISP).

- C. Through a public IP address, you can access another computer on the Internet, such as a Web server.
- D. The ranges of public IP addressing are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.
- E. Private addresses are allocated by the Internet Assigned Numbers Authority (IANA).

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Public addresses are publicly registered with the Internet Assigned Numbers Authority (IANA). Through a public IP address, you can access an Internet computer like a Web server.

The following statements are true of public IP addressing:

- These addresses are publicly registered with the Internet Assigned Numbers Authority (IANA)
- Through a public IP address, you can access another Internet computer, such as a Web server.
- Other people on the Internet can obtain information about or access to your computer via a public IP address. ▪

Public IP addresses are visible to the public.

The option stating that public IP addresses are publicly registered with the Internet Service Provider (ISP) is incorrect. Public IP addresses are registered with the Internet Assigned Numbers Authority (IANA). Since 1998, InterNIC has been primarily responsible for allocating domain names and IP addresses under the governance of the Internet Corporation for Assigned Names and Numbers (ICANN) body, a U.S. non-profit corporation that was created to oversee work performed by the Internet Assigned Numbers Authority (IANA).

The option stating that 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255 are the range of public IP addressing is incorrect. These ranges belong to private IP addressing.

The option stating that private addresses are allocated by the IANA is incorrect. Private IP address are not managed, but are used by private organizations as they see fit.. The IANA is governed by ICANN, and its primarily role is to allocate overseas global IP addresses from the pools of unallocated addresses, as well as DNS root zone management.

Objective:

Network Fundamentals Sub-

Objective:

Describe the need for private IPv4 addressing

References: <http://www.debianadmin.com/private-and-public-ip-addresses-explained.html>

QUESTION 71

Which type of network uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as an access method?

- A. Token Ring
- B. LocalTalk
- C. 100VG-AnyLan
- D. Ethernet

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Ethernet networks use CSMA/CD as an access method. In CSMA/CD, if a device wants to send a frame in the network, it first determines if the network is free. If the network is not free, the node will wait before sending the frame into a network. If the network is free, it sends the frame; if another device sends a frame simultaneously then their signals or frames collide. When the collision is detected, both packets wait for a random time before retrying.

The following statements are true regarding CSMA/CD:

- CSMA/CD is required for shared collision domains, such as when hosts are connected via hubs. (Hubs are Layer 1 devices, and thus do not create collision domains.)
 - CSMA/CD networks normally operate in half-duplex mode, since in a shared collision domain, a host cannot send and receive data at the same time. ▪
- CSMA/CD is not required when connected to non-shared (private) collision domains, such as when hosts are connected to dedicated switch ports. ▪
- Switches create dedicated collision domains, so devices can operate in full-duplex mode.

Token Ring is incorrect because Token Ring uses token passing as the access method.

LocalTalk is incorrect because LocalTalk uses CSMA/CA (Collision Avoidance) as the access method.

100VG-AnyLan is incorrect because 100VG-AnyLan uses demand priority as the access method.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Interpret Ethernet frame format

References:

[Cisco > Internetworking Technology Handbook > Introduction to LAN Protocols > LAN Media-Access Methods](#)

QUESTION 72

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:

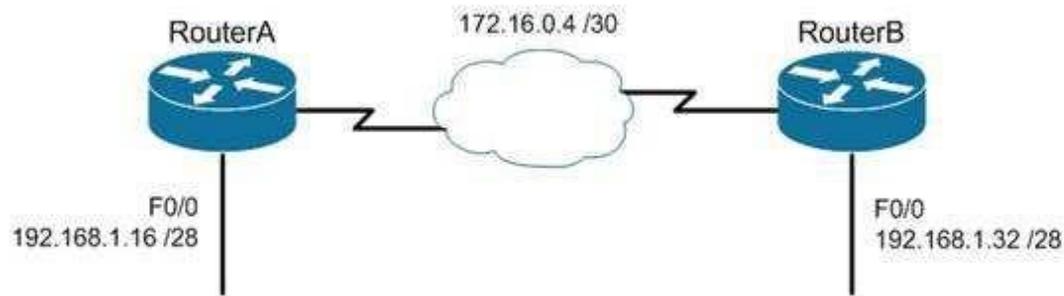
Describe WAN access connectivity options

References:

[Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies > DSL](#)

QUESTION 73

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 74

You and your team are evaluating the use of OSPFv3 in your IPv6 network.

Which of the following statements is true of OSPFv3?

- A. There will be a higher demand on the processor to run the link-state routing algorithm
- B. Router IDs must match for adjacency formation
- C. Area IDs do not need to match for adjacency formation
- D. Area types do not need to match for adjacency formation

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

There will be a higher demand on the processor to run the link-state routing algorithm. As with OSPFv2, OSPFv3 uses the Shortest Path first (SPF) algorithm, which is processor intensive. It is one of the only downsides of using the algorithm.

OSPFv3 also shares a number of other characteristics with its v2 counterpart with respect to adjacency formation. For example: ▪

Router IDs should not match.

- Router IDs should reflect the correct router ID for each device.
- Area IDs must match.
- Area types must match.

Objective:

Routing Fundamentals Sub-

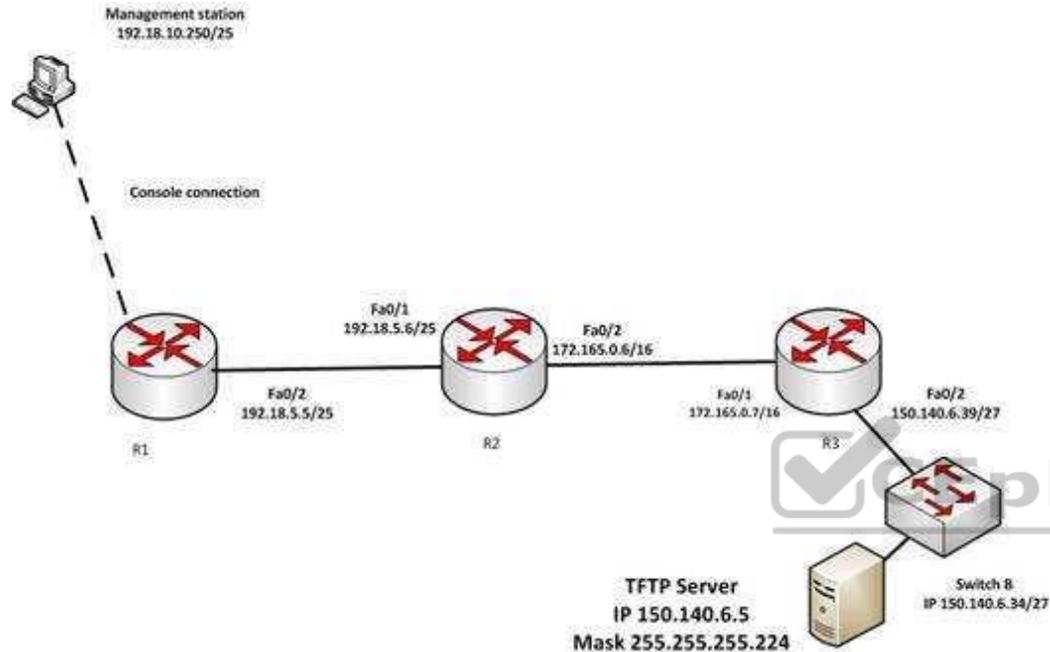
Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

QUESTION 75

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 R1 and 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:

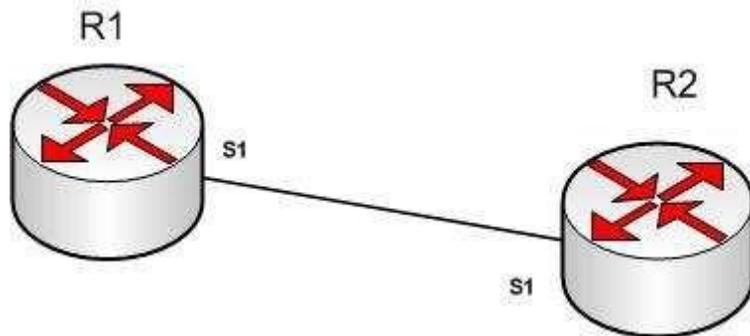
Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

[Cisco > Support > IP Routing > Design TechNotes > Document ID: 13788 > IP Addressing and Subnetting for New Users](#)

QUESTION 76

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 R2
R1(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 77

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 78

Which Cisco Internetwork Operating System (IOS) command would be used to set the privileged mode password to "cisco"?

- A. `router(config)# enable password cisco`
- B. `router# enable secret cisco`
- C. `router(config)# line password cisco`
- D. `router(config-router)# enable password cisco`



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The `enable password` command is used to set the local password to control access to privileged levels. This command is executed on the global configuration mode, as in `router(config)# enable password cisco`. The syntax of the command is:

`router(config)# enable password [level level] {password | [encryption-type] encrypted-password}`

The parameters of the command are as follows:

- `level level`: An optional parameter to set the privilege level at which the password applies. The default value is 15.
- `password`: Specifies the password that is used to enter enable mode.
- `encryption-type`: An optional parameter to specify the algorithm used to encrypt the password.
- `encrypted-password`: Specifies the encrypted password that is copied from another router configuration.

The `router# enable secret cisco` command is incorrect because the `enable secret` command must be executed from global configuration mode, not privileged EXEC mode. In fact, this is the password for which you will be prompted when you attempt to enter privilege exec mode.

The line password command is incorrect because this command is not a valid Cisco IOS command.

The router(config-router)# enable password cisco command is incorrect because the enable password command must be entered in global configuration mode.

Objective:

Infrastructure Security Sub-

Objective:

Configure, verify, and troubleshoot basic device hardening

References:

[Cisco > Cisco IOS Security Command Reference > E > enable password](#)

[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 79

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 80

From which of the following attacks can Message Authentication Code (MAC) shield your network?

- A. DoS
- B. DDoS
- C. spoofing
- D. SYN floods



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Message Authentication Code (MAC) can shield your network from spoofing attacks. Spoofing, also known as masquerading, is a popular trick in which an attacker intercepts a network packet, replaces the source address of the packets header with the address of the authorized host, and reinserts fake information which is sent to the receiver. This type of attack involves modifying packet contents. MAC can prevent this type of attack and ensure data integrity by ensuring that no data has changed. MAC also protects against frequency analysis, sequence manipulation, and ciphertext-only attacks.

MAC is a secure message digest that requires a secret key shared by the sender and receiver, making it impossible for sniffers to change both the data and the MAC as the receiver can detect the changes.

A denial-of-service (DoS) attack floods the target system with unwanted requests, causing the loss of service to users. One form of this attack generates a flood of packets requesting a TCP connection with the target, tying up all resources and making the target unable to service other requests. MAC does not prevent DoS attacks. Stateful packet filtering is the most common defense against a DoS attack.

A Distributed Denial of Service attack (DDoS) occurs when multiple systems are used to flood the network and tax the resources of the target system. Various intrusion detection systems, utilizing stateful packet filtering, can protect against DDoS attacks.

In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. A SYN flood attack is a type of denial of service attack that exploits the buffers of a device that accept incoming connections and therefore cannot be prevented by MAC. Common defenses against a SYN flood attack include filtering, reducing the SYN-RECEIVED timer, and implementing SYN cache or SYN cookies.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

[Cisco > The Internet Protocol Journal, Volume 10, No. 4 > IP Spoofing](#)

QUESTION 81

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 ROMMON 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 82

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:

$$\text{Metric} = \left[\frac{K1 * \text{Bandwidth} + (K2 * \text{Bandwidth}) / (256 - \text{load}) + K3 * \text{Delay}}{K5 / (\text{reliability} + K4)} \right]$$

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 83

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](#)

QUESTION 84

Which Cisco Internetwork Operating System (IOS) command is used to save the running configuration to non-volatile random access memory (NVRAM)?

- A. copy startup-config running-config
- B. move startup-config running-config
- C. copy running-config startup-config
- D. move startup-config running-config

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The copy running-config startup-config command is used to save the running configuration to NVRAM. This command will should always been run after making changes to the configuration. Failure to do so will result in the changes being discarded at the next restart of the router. When the router is restarted, the startup configuration file is copied to RAM and becomes the running configuration.

The copy startup-config running-config command is incorrect because this command is used to copy the startup configuration to the running configuration. The command would be used to discard changes to the configuration without restarting the router.

The move startup-config running-config and move startup-config running-config commands are incorrect because these are not valid Cisco IOS commands. There is no move command when discussing the manipulation of configuration files.

Objective:

Infrastructure Management Sub-

Objective:

Perform device maintenance

References:

[Cisco Documentation > RPM Installation and Configuration > IOS and Configuration Basics](#)

QUESTION 85

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 86

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 87

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:

$$2^n - 2 = x$$

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:

$$\text{Number of hosts} = 2^6 - 2$$

$$\text{Number of hosts} = 64 - 2 = 62$$

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:

11111111.11111111.11111111.11000000

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 $2^5 - 2 = 32$.

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 $2^7 - 2 = 128$.

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 88

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 Switch 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 89

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-

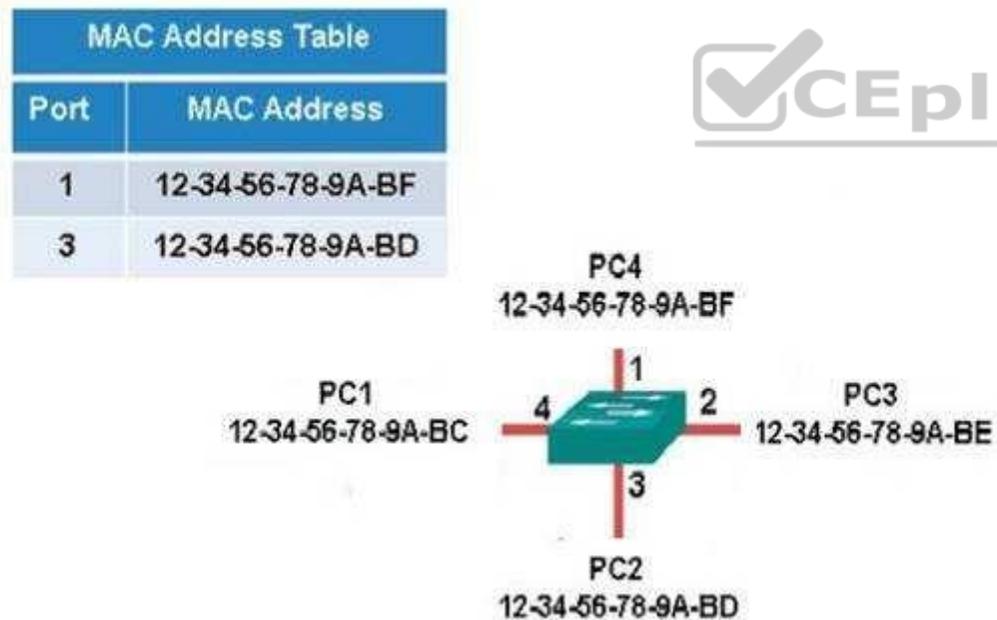
Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

QUESTION 90

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



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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The frame with a source MAC of 12-34-56-78-9A-BF and a destination MAC 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 91

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
```

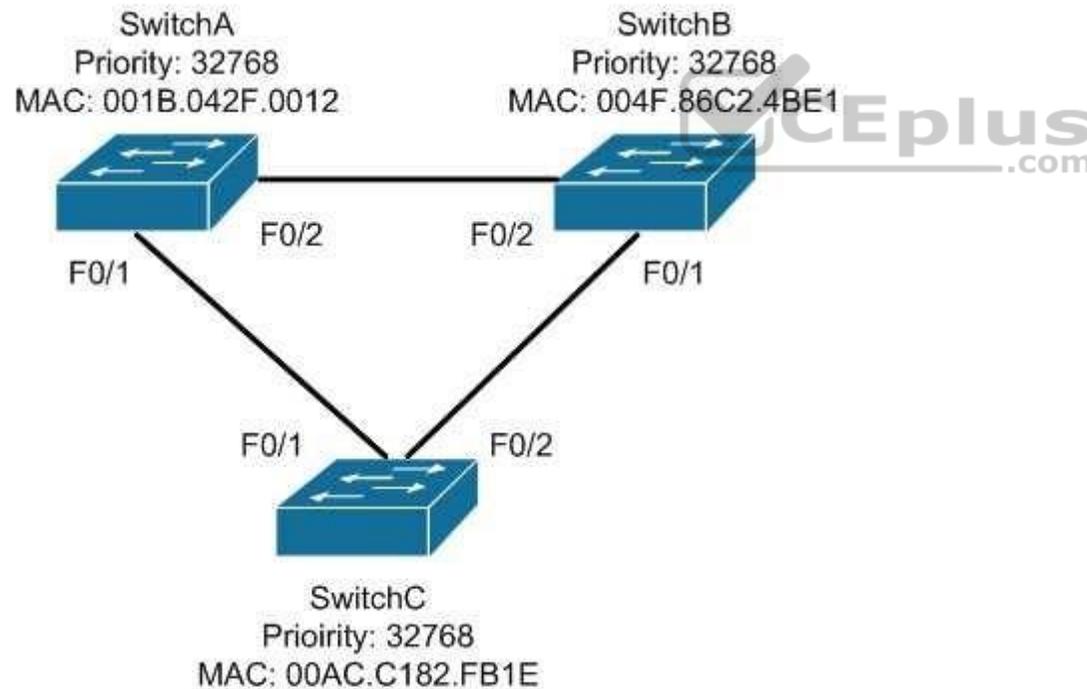
```
database switchB(vlan)#  
vtp server switchB(vlan)#  
vlan 50
```

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](http://www.cisco.com/c/en/us/press/home/articles/cisco-certification/ccna/ccna-self-study-icnd-exam/extending-switched-networks-with-virtual-lans.html)

QUESTION 92

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 93

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:

QUESTION 94

Which Cisco Internetwork Operating System (IOS) command would be used to define a static route for network 192.168.11.0 through default gateway 192.168.43.1?

- A. router(config)# ip route 192.168.11.0 255.255.255.0 192.168.43.1
- B. router# ip route 192.168.11.0 255.255.255.0 192.168.43.1
- C. router(config)# ip classless 192.168.43.1
- D. router(config)# ip default gateway 192.168.11.0 255.255.255.0 192.168.43.1
- E. router# ip default gateway 192.168.43.1

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

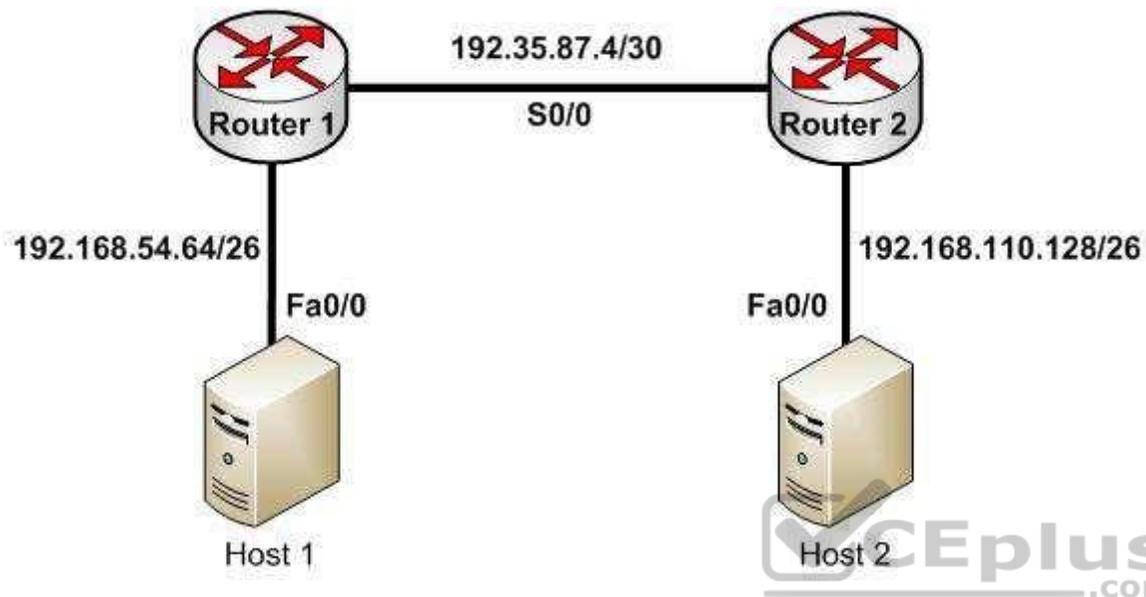
The router(config)# ip route 192.168.11.0 255.255.255.0 192.168.43.1 command would be used to define a static route for network 192.168.11.0 through default gateway 192.168.43.1. Static routing is used to manually configure routes to remote networks. The syntax of the ip route command is as follows:

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

The parameters 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): Static routes have an AD of 1, which can be changed to change the priority of the route.

Static routing is often implemented in small yet stable networks where the number of routes is small and manageable, and the network can benefit from the elimination of the traffic that dynamic routing protocols would introduce. If this is the case, it is important that all routes be statically created, or else networking problems can occur. For example, if in the diagram below no route to the 192.168.110.128/26 network on Router 2 exists on Router 1, Host 1 will be unable to ping Host 2. The fact that Host 1 would still be able to ping the S0/0 interface on Router 2 could obscure this missing route.



Host 1 will be able to ping the S0/0 interface of Router 2 because the 192.35.87.4/30 network will be in the routing table of Router 1, being directly connected to Router 1. Directly connected routes are automatically placed in the routing table. However, if you executed the show run command on Router 1, the output would indicate that no route to the 192.168.110.128/26 exists:

```
<output omitted> interface Fa0/1      ip
address 192.168.54.65 255.255.255.192    no
shutdown interface S0/0      ip address
192.35.87.5 255.255.255.252          no shutdown
```

The option `router# ip route 192.168.11.0 255.255.255.0 192.168.43.1` is incorrect because the `ip route` command should be configured in the global configuration mode.

The option `router(config)# ip classless 192.168.43.1` is incorrect because the `ip classless` global configuration mode command allows a router to accept and forward packets for subnets that are not directly connected. The packets are forwarded to the best available supernet route.

The option `router(config) # ip default gateway 192.168.11.0 255.255.255.0 192.168.43.1` is incorrect because the `ip default gateway` command is used to define the default gateway address when IP routing is disabled in the network.

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](#)
[Cisco > Cisco IOS IP Routing Protocols Command Reference > IP Routing Protocol-Independent Commands: A through R > ip route](#)

QUESTION 95

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 96

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 97

Which Cisco IOS command enables a router to copy IOS images to a router?

- A. copy tftp flash
- B. copy flash tftp
- C. copy running-config tftp
- D. copy running-config startup-config
- E. copy tftp running-config

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The copy tftp flash command enables a router to copy an IOS image (the router operating system) to a router from a TFTP server. One router can act as a TFTP server to the other in this process.

The following example illustrates the steps to copy an image from Router A to Router B:

- Verify the connectivity between Router A and Router B using the ping command.
- Check the image size on both of the routers with the show flash command to verify that enough space exists on Router B.
- Configure Router A as the TFTP server using the configure terminal command. Use the tftp-server flash [partition-number:]filename1 [alias filename2] [accesslist-number] command to define the path to system image that needs to be transferred. There can be multiple entries for multiple images.
- Copy the image from Router A to Router B using the copy tftp flash command.
- Verify the flash for the copied new image on Router B with the show flash command.

The copy flash tftp command is used to copy an IOS image from the router to a TFTP server.

The copy running-config tftp command is used to copy the active or running configuration file from RAM to a TFTP server.

The copy running-config startup-config command copies the active or running configuration from RAM to NVRAM. This command creates the configuration file that will be used as the startup configuration at reboot. This should always be done after making changes to the router so that the changes are saved when the router is rebooted.

The copy tftp running-config command merges a backup configuration with the currently active running configuration in RAM.

Objective:

Infrastructure Management Sub-

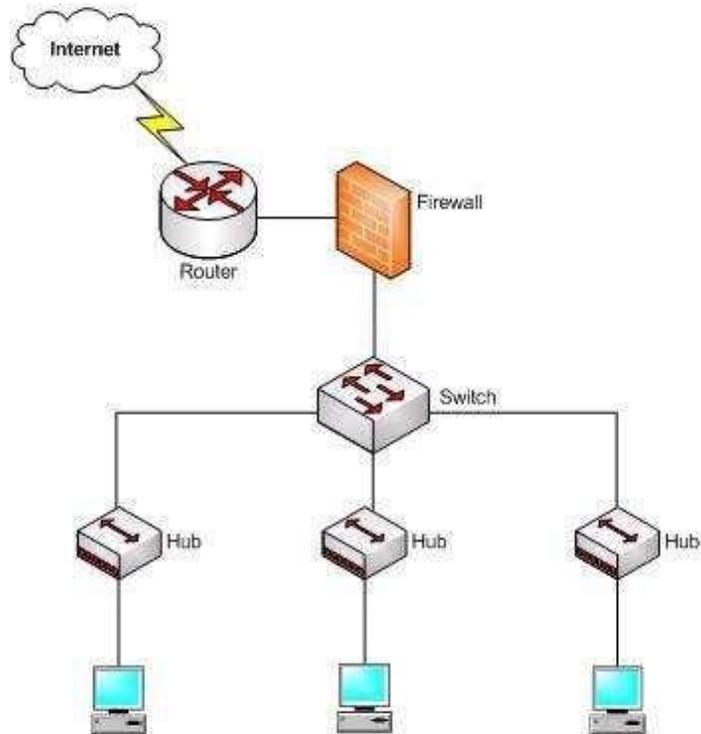
Objective:

Perform device maintenance

References:

QUESTION 98

Which device in the given network diagram has as its primary responsibility the regulation of network traffic flow based on different trust levels for different computer networks?



- A. the router
- B. the switch
- C. the hub(s)
- D. the firewall

Correct Answer: D Section: (none) Explanation

Explanation/Reference:

Explanation:

The firewall has as its primary responsibility the regulation of network traffic flow based on different trust levels for different computers or networks. In the network diagram shown in the exhibit, a firewall protects the network from unauthorized access attempts. A firewall can be implemented in hardware or software. Firewalls permit, deny, or filter data packets coming into and going out of the network. This helps prevent unauthorized access attempts from outside the network.

The primary function of a router is to perform routing between two subnets or between dissimilar network technologies. Routers can provide limited firewall functionality, but a firewall is a dedicated hardware or software solution with the primary responsibility of securing the network. A router does not have as its primary responsibility the regulation of network traffic flow based on different trust levels.

Switches work at Layer 2 in the Open System Interconnection (OSI) model and perform the function of separating collision domains. A switch does not have as its primary responsibility the regulation of network traffic flow based on different trust levels.

A hub is a device that provides a common connection point for network devices. The primary responsibility of a hub is not to regulate network traffic flow based on different trust levels.

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 99

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 100

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 101

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 25Router5(config)# network 192.168.5.0
- B. Router5(config)#ipv6 ospf 25Router5(config)#router-id 192.168.5.1
- C. 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
D. Router5(config)#ipv6 unicast-routing
Router5(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 102

What is the significance of the following BECN packet statistics?

```
Router# show frame-relay pvc 16
```

```
PVC Statistics for interface serial0 (Frame Relay DTE)
```

```
DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0
```

```
input pkts 0 output pkts 0 in bytes 0
```

```
out bytes 0 dropped pkts 0 in FECN pkts 0
```

```
in BECN pkts 100 out FECN pkts 0 out BECN pkts 0
```

```
<<output omitted>>
```

- A. The router is experiencing congestion in sending frames.
- B. The router is experiencing congestion in receiving frames.
- C. The Frame Relay mapping table is missing an entry.
- D. The Frame Relay mapping table is corrupt.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When frames arrived at a router with the Backwards Explicit Congestion Notification (BECN) bit set, congestion was encountered in the opposite direction from which the frame was traveling. This bit is set by the Frame Relay switch. If an incoming packet has the BECN bit set, then this indicates congestion in outgoing packets, so the router will experience congestion in sending frames.

When a Frame Relay switch encounters congestion, it will mark packets being sent in both directions on a PVC with either the Forward Explicit Congestion Notification (FECN) or the BECN bit set. It will set the BECN bit on packets headed in the opposite direction of the congestion and FECN in the same direction as the congestion. When a packet with the FECN bit is received by a router, it means there will be congestion when the receiving router receives packets.

A third type of marking is the Discard Eligibility (DE) bit. When this bit is set on a packet, it ensures that if congestion occurs and packets need to be discarded, the packet with the DE bit set should be discarded first. ALL packets in excess of the committed information rate (CIR) are marked with the DE bit.

Frame Relay mapping tables have nothing to do with congestion in the Frame Relay network.

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

References:

[Cisco > Home > Support > Technology Support > WAN > Frame Relay > Design > Design TechNotes > show Commands for Frame Relay Traffic Shaping](#)

QUESTION 103

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 104

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 105

Which of the following fields are in a Transmission Control Protocol (TCP) header? (Choose three.)

- A. Length
- B. Sequence Number
- C. Data Offset
- D. Type-of-Service
- E. Window

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

- Sequence Number, Data Offset, and Window are the fields found in a TCP header. TCP hosts create a connection-oriented session with one another. The following are the fields found in a TCP header:
 - Sequence Number: Refers to the first byte of data in the current message. This field helps TCP to reassemble the packets in the correct order. For example, when data is transferred between an FTP server and FTP client, the receiver uses this field to reassemble the packets into the original file.
 - Data Offset: Refers to the number of 32-bit words in the TCP header.
 - Window: Refers to the size of the available space for the incoming data.
 - Source Port and Destination Port: Refer to the point where upper-layer source and destination processes receive TCP services. Both TCP and UDP packets contain these fields.
 - Acknowledgment Number: Refers to the sequence number of the next byte of data which the sender will receive.
 - Reserved: Reserved for future use.
 - Flags: Contains control information, such as the SYN and ACK bits which are used to establish and acknowledge communication, and the FIN bit which is used to terminate the connection.
 - Checksum: An indicator of any damage to the header while being in transit. Both TCP and UDP packets contain this field.
 - Urgent Pointer: Refers to the first urgent data byte in the packet.
 - Options: Used to specify TCP options. Only TCP packets contain this field.
- Data: Has upper-layer information.

TCP is used for unicast transmissions and provides connection -oriented services for upper layer protocols. It will establish a state of connection between two devices before any data is transferred; for example, before a workstation can exchange HTTP packets with Web server, a TCP connection must be established between the workstation and the Web server.

The Length field is found in a User Datagram Protocol (UDP) header, where it specifies the length of the UDP header and data. UDP headers contain the Source Port, Destination Port, Length, and Checksum fields.

Sequence number, acknowledgment number, and windows size are 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, which refers to the number of packets that can be received without an acknowledgment.

The Type-of-Service field is found in an Internet Protocol (IP) header, where it specifies the handling of a current datagram by an upper-layer protocol.

Objective:

Network Fundamentals Sub-

Objective:

Compare and contrast TCP and UDP protocols

References:

[Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Internet Protocols > TCP Packet Format](#)

QUESTION 106

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 107

Which two are NOT valid Cisco IOS commands used for Cisco Discovery Protocol (CDP)? (Choose two.)

- A. show cdp
- B. show cdp entry *
- C. show cdp neighbor entries



<https://vceplus.com/>



- D. show cdp neighbors detail
- E. show cdp devices

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show cdp neighbor entries command and the show cdp devices command are not valid Cisco IOS commands.

The Cisco IOS commands used for CDP are as follows:

show cdp: This command is used to view global CDP information, such as timer and hold time.

show cdp entry *: This command is used to view information regarding all neighboring devices.

show cdp neighbors detail: This command is used to view the details regarding the neighboring devices which are discovered by the CDP. This 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]
```

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 108

What data structure is pictured in the graphic?

0-15	16-31
Source Port Number	Destination Port Number
Length	Checksum
Data	



- 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).

Bit 0		Bit 15		Bit 16		Bit 31	
Source Port (16)				Destination Port (16)			
Sequence Number (32)							
Acknowledgement Number (32)							
Header length (4)		Reserved		Code Bits (6)		Window (16)	
Checksum (16)				Urgent (16)			
Options (0 or 32 if any)							
Data (Varies)							

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 109

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 284244 via
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
2248564 via Connected, Serial0/0
- C. 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
- D. P 172.16.60.0/24, 1 successors, FD is
2248564 via 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 110

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 111

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 112

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-config]?
```

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 is 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](#)

QUESTION 113

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 114

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 115

Which technique is used to stop routing loops by preventing route update information from being sent back over the interface on which it arrived?

- A. Holddown timer

- B. Triggered updates
- C. Route poisoning
- D. Split horizon
- E. Maximum hop count

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Split horizon stops routing loops by preventing route update information from being sent back over the interface on which it arrived. Routing loops can occur due to slow convergence and inconsistent routing tables, and can cause excessive use of bandwidth or even complete network failure. Split horizon can prevent routing loops between adjacent routers.

Holddown timers prevent regular update messages from reinstating a route that is unstable. The holddown timer places the route in a suspended, or "possibly down" state in the routing table, and regular update messages regarding this route will be ignored until the timer expires.

Triggered updates are sent as soon as a change in network topology is discovered, as opposed to waiting until the next regular update interval (every 30 seconds in RIP networks). This speeds convergence and helps prevent problems caused by outdated information.

Route poisoning "poisons" a failed route by increasing its cost to infinity (16 hops, if using RIP). Route poisoning is combined with triggered updates to ensure fast convergence in the event of a network change.

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 116

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 117

Examine the following partial output of the show interfaces command.

```
Router# show interfaces ethernet 0/0
Ethernet0/0 is administratively down, line protocol is down
Hardware is AmdP2, address is 0003.e39b.9220 (bia 0003.e39b.9220)
Internet address is 10.1.0.254/16
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
<<output omitted>>
```

Which of the following statements are true? (Choose all that apply.)

- A. the interface is functional
- B. the largest frame allowed through this connection is 1500 bytes
- C. the interface needs the no shutdown command executed to be functional
- D. the largest frame allowed through this connection is 10000 Kbs

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

From this output, we can determine that the largest frame allowed through this connection is 1500 bytes and that the interface needs the no shutdown command executed to be functional. The portions of the output that tell us this are:

MTU 1500 bytes indicates that the Maximum Transmission Unit (MTU) is 1500 bytes. The MTU is the largest frame size allowed.

Ethernet0/0 is administratively down indicates that the interface has either been disabled or has never been enabled. The command no shutdown is used to enable an interface, and until enabled, it will not function.

The interface is not functional, as indicated by the Ethernet0/0 is administratively down portion of the output.

The largest frame allowed through this connection is not 10000 Kbs. It is 1500 bytes. It is interesting to note that the bandwidth of the connection is 10000 Kbs, as indicated by the section:

BW 10000 Kbit

Objective:

LAN Switching Fundamentals Sub-

Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

QUESTION 118

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 if 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 119

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 120

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 121

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 122

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 123

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)

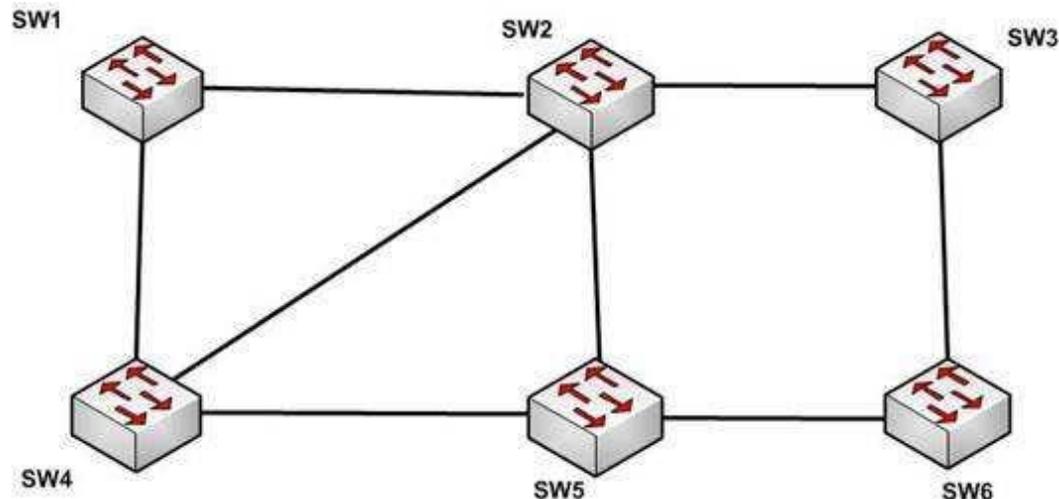
Explanation

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 parts.

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 124

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) point-to-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 125

Examine the following output from SwitchD.

```
switch# show interfaces fastethernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<<output omitted>>
```

Based on this output, what command MUST be executed for an 802.1q trunk to be created on port Fa0/1?

- A. switchport mode trunk
- B. switchport mode nonegotiate
- C. switchport trunk encapsulation 802.1q
- D. switchport trunk native VLAN



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The command switchport mode trunk must be executed for a trunk to form. The output indicates that the Administrative Mode of the port is "static access," which means the port has been configured as a static (fixed) access port. Access mode disables trunking on an access port.

Below is a sample of the configuration required to allow a router to provide inter-VLAN routing between two VLANs residing on the switch:

```
Router(config)#interface fa0/0
Router(config)#no shut down
Router(config)#interface fa0/0.1
Router(config-subif)#encapsulation dot1q
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config)#interface fa0/0.2
Router(config-subif)#encapsulation dot1q
Router(config-subif)#ip address 192.168.20.1 255.255.255.0

Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
```

For this example, the following statements are true:

- The trunk link connects to Fa0/0 on the router and Fa0/1 on the switch.
- The physical interface F0/0 on the router has been divided into two subinterfaces, Fa0/0.1 and Fa0/0.2.
- The encapsulation type of 802.1q has been specified on the two subinterfaces of the router.
- The physical interface on the switch has been specified as a trunk link.
- The IP addresses 192.168.10.1 and 192.168.20.1 should be the default gateways of the computers located in VLANs 1 and 2, respectively.

The switchport mode nonegotiate command does not need to be executed because the switch is already configured for non-negotiation, as indicated by the output Negotiation of Trunking: Off. Trunk negotiation using the Dynamic Trunking Protocol (DTP) does not need to be enabled for a trunk to form.

The switchport trunk encapsulation 802.1q command does not need to be executed for a trunk to form. Also, the output Operational Trunking Encapsulation: dot1q indicates that 802.1q encapsulation is already configured.

The switchport trunk native VLAN command does not need to be executed. This command is used to change the native VLAN from its default of 1, but leaving it set to the default of 1 will not prevent the trunk from forming.

Objective:
Routing Fundamentals

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

References:

[Cisco > Catalyst 3560 Switch Software Configuration Guide, Rel. 12.2\(25\)SEE > Configuring VLANs > Configuring VLAN Trunks > Trunking Overview](#)

QUESTION 126

As you are training a new junior technician, the trainee is examining the routing table. He tells you that there are four different routes to the same network in different routing databases. He asks you which of the routes will be used to populate the routing table.

What will your answer be, assuming that all routing protocols are set at the default administrative distance?

- A. The route with an R next to it
- B. The route with an S next to it
- C. The route with a C next to it
- D. The route with an I next to it

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

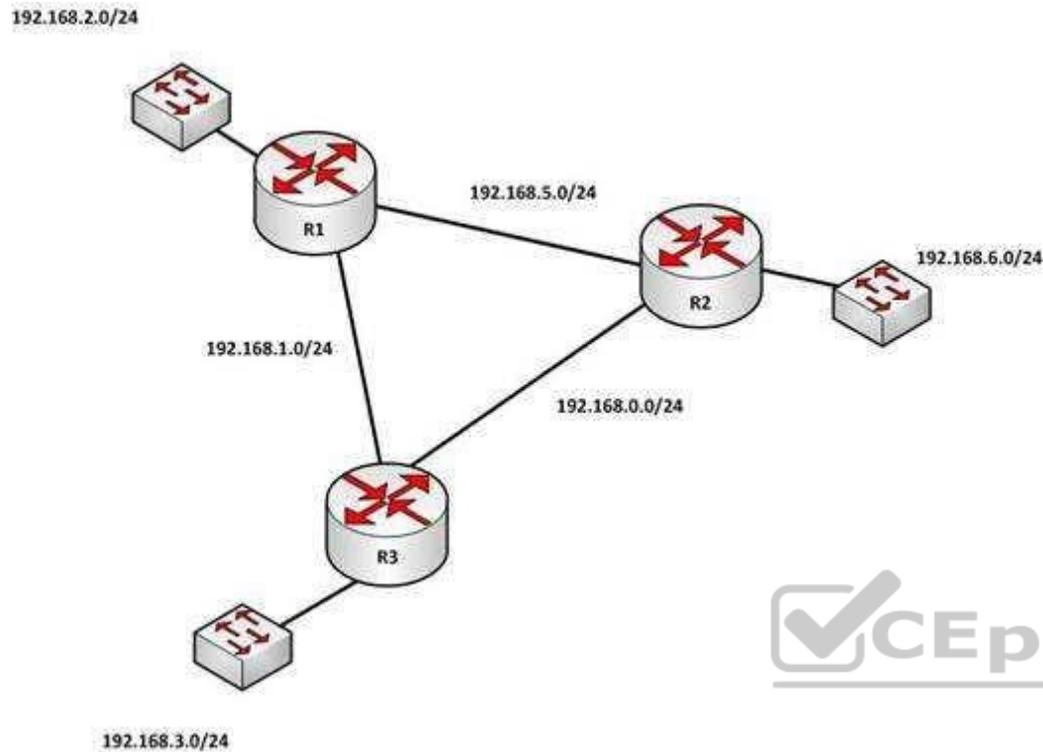
Explanation:

The route with a C next to it is a directly connected route and has an administrative distance of 0, which means it will be preferred over any routes with a larger value for administrative distance. Each routing protocol has a default administrative distance assigned. Administrative distance is used by the router to determine the preferred route when a route is learned from different routing protocols. This process can be manipulated by the administrator by using the distance command to alter the default assignments.

It is significant to note that routers with no static routes and no routing protocols enabled will populate all directly connected routes to the routing table with no action on the part of the administrator. Routes that are NOT directly connected will not be in the routing table unless one of two things occurs:

- A static route is created by the administrator
- A routing protocol is enabled that allows the router to learn about the network and its route from another router running the same routing protocol

For example, in the diagram below, R3 will have routes to the 192.168.3.0/24 ,192.168.1.0/24 and the 192.168.0.0/24 networks in its routing table by default. It will only have routes to the 192.168.2.0/24, 192.168.5.0/24, and 192.168.6.0/24 networks if a routing protocol is used or if an administrator creates static routes for each network.



When a packet is received by a router interface, the router de-encapsulates the frame or removes the layer two information (MAC data for Ethernet or DLCIs for frame relay) and then performs a lookup for the network ID of the network in which the destination IP address resides. When multiple routes exist, it will choose the one with the lowest administrative distance. The router only places the route with the lowest distance in the table.

The route with an R next to it is a route learned from Routing Information Protocol (RIP). It has a default administrative distance of 120, so it will not prefer over a directly connected route.

The route with an S next to it is a static route or one configured manually. It has an administrative distance of 1, so it will not be preferred over a directly connected route.

The route with an I next to it is a route learned from Internal Gateway Routing Protocol (IGRP). It has an administrative distance of 100, so it will not be preferred over a directly connected route.

Objective:

Routing Fundamentals Sub-

Objective:

Interpret the components of routing table

References:

[Cisco > Support > IP > IP Addressing Services > Design Technotes > What Is Administrative Distance? > Document ID: 15986](#)

QUESTION 127

What command can be used on a Cisco switch to display the virtual MAC address for the HSRP groups of which the switch is a member?

- A. switch# show standby mac
- B. switch# show hsrp mac
- C. switch# show standby
- D. switch# show standby brief

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The command show standby can be used to display the virtual MAC address for HSRP groups of which a switch is a member. 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 standby switch will take over as the active switch if the timer expires before it hears a heartbeat from the active switch. Below is an example of the show standby command for the HSRP group 1:

```
Tacoma# show standby
```

```
Fastethernet0/1 - group 1
  State is active
    3 state changes, last state change 00:22:49
  Virtual IP address is 192.168.5.3
    Secondary virtual ip address 192.168.5.3
  Active virtual MAC address is 0006.6b45.5801
    Local virtual MAC address is 0006.6b45.5812(bia)
  Hello time is 4 sec, hold time 12 sec
    Next hello sent in 1.664 sec
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is unknown expired
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
    Down Interface Fastethernet0/2, pri 15
    Down Interface Fastethernet0/3
  IP redundancy name is "HSRP1", advertisement interval is 34 sec
```

In the above output, the following can be determined:

- The router is currently active for the group, as can be seen in line 2. The Active Virtual MAC address is 0006.6b45.5801, which includes the group number (1) in the last two positions, which is why the address is different from the routers actual MAC address shown on the next line. Special Note: Some router models (Cisco 2500, 4000 and 4500) WILL NOT use this altered MAC address format, but will instead use the real MAC address for the virtual MAC address and will display that MAC address as the virtual MAC address in the output of the show standby command. An example of the output of the show standby command on an older router such as the 2500 would be as follows:

```
Router# show standby
Ethernet0/1 - Group 1
State is Active
  2 state changes, last state change 00:30:59
Virtual IP address is 10.1.0.20
Secondary virtual IP address 10.1.0.21
Active virtual MAC address is 0004.4d82.7981
Local virtual MAC address is 0004.4d82.7981 (bia)
```

These routers have Ethernet hardware that only recognize a single MAC address. In either case, if for some reason this router becomes the standby router, such as due to loss of interfaces, then when the interfaces come back up it will be able to recover the active role because it is set for preemption, as shown on line 10. The router is tracking two of its own interfaces. Because both interfaces are down, the router's priority has been reduced by 25 (15 for Fastethernet0/2 and 10 for Fastethernet0/3), from the configured value of 120 to 95. This data is shown on lines 13-16. The default is 10 if not otherwise specified, as is the case for Fastethernet0/3.

- If either of the two interfaces comes back up, the priority will be increased by the amount assigned to the interface. For example, if Fastethernet0/3 comes back up, the priority will become 105 (95 + 10).
- The standby router is unreachable, which can be determined because it is marked unknown expired in line 12. This could be due to either a physical layer issue or an HSRP misconfiguration.

The command `show standby brief` can be used to view summary information about HSRP groups of which the switch is a member. This information includes the group number, priority, state, active device address, standby address, and group address. It does not include the virtual MAC address.

The commands `show standby mac` and `show hsrp mac` are invalid 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 128

Which of the following statements are NOT true, based on the output below?

```
Access1#show spanning-tree vlan 10
```

```
VLAN0010
```

```
Spanning tree enabled protocol rstp
```

```
Root ID Priority 24586
```

```
Address 0015.63f6.b700
```

```
Cost 19
```

```
Port 107 (FastEthernet3/0/1)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
```

```
Address 000f.f794.3d00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Fa3/0/1 Root FWD 19 128.107 P2p
```

```
Fa3/0/2 Altn BLK 19 128.108 P2p  
-----
```



- A. This switch is the root bridge.
- B. This switch has a priority of 32778.
- C. This switch has a MAC address of 0015.63f6.b700.
- D. All ports will be in a state of discarding, learning, or forwarding.
- E. All designated ports are in a forwarding state.
- F. This switch is using the default priority for STP

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The upper half of the output provides information about the root bridge. It indicates that the root bridge has a bridge priority of 24586 and a MAC address of 0015.63f6.b700. The bottom half of the output pertains to the current switch, and indicates that this switch has a bridge priority of 32778 and a MAC address of 000f.f794.3d00.

The value of the switch bridge priority is arrived at by adding the configured priority of 32768, which is indicated by the line priority 32768 sys-id-ext 10, to the VLAN ID of 10. Because 32768 is the default bridge priority for STP, this switch is set to the default priority for STP.

The priority of this switch is 32778. The bridge priority is arrived at by adding the configured priority of 32768 to the VLAN ID of 10.

This switch is not the root bridge, as indicated by the differences in priorities and MAC addresses between the root ID and the bridge ID output. If this were the root bridge, the MAC addresses and priority values would be the same in both the Root ID and the Bridge ID sections.

Finally, when a switch is using RSTP, as indicated by the output Spanning tree enabled protocol rstp, all ports will be in a state of discarding, learning, or forwarding, with all designated ports in a forwarding state. When RSTP has converged, all ports will be in either the discarding or forwarding states.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot STP protocols

References:

[Cisco > Cisco IOS Bridging Command Reference > show spanning-tree](#)



QUESTION 129

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 130

On which of the following networks will OSPF elect a designated router (DR)? (Choose two.)

- A. Broadcast
- B. NBMA
- C. Point-to-point
- D. Point-to-multipoint

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

OSPF will perform an election for a designated router (DR) and backup designated router (BDR) on every multi-access network segment. Multi-access segments are defined as segments where more than two hosts can reach each other directly, such as a shared Ethernet segment (broadcast multi-access) or Frame Relay (non-broadcast multi-access, or NBMA).

DR and BDR elections do not occur on point-to-point or point-to-multipoint segments. Point-to-point and point-to-multipoint segments are not considered multiaccess segments. OSPF routers on these network types will establish an adjacency without a DR/BDR election.

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 131

A new trainee is setting up a router in a test lab, and he asks you to describe the use of the connector marked BRI on the router.

Which is a correct use for this connector?

- A. A WAN interface for a T1 connection
- B. A LAN interface to connect to a switch
- C. An interface to connect a console cable
- D. A WAN interface for an ISDN connection

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Explanation:

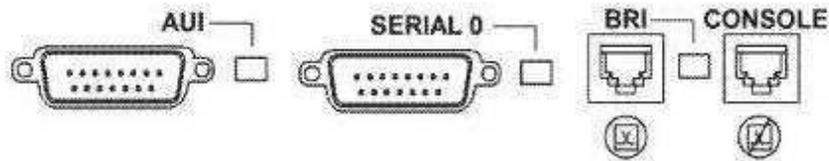
The connector marked BRI is used for an Integrated Services Digital Network (ISDN) connection, specifically a basic rate interface (BRI). An ISDN basic rate interface provides three channels: a D channel for control signaling, and two B or bearer channels for data, resulting in 128 bits of bandwidth.

A WAN interface for a T1 connection would be connected to a serial port on the router, not the BRI interface. It would not accept a basic rate ISDN connection.

A LAN interface to connect to a switch would be an Ethernet connection that used either an RJ-45 connector or a legacy AUI connector. It would not accept a basic rate ISDN connection.

An interface to a console connector will look like an RJ-45 Ethernet connector but will only accept a console or rollover cable, and is used to manage the router. It would not accept a basic rate ISDN connection.

These various ports can be seen on the backplane of a router as shown below:



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

References:

[http://www.tutorialsweb.com/networking/routers/cisco-routers-ios.htm#Hardware%20Components:](http://www.tutorialsweb.com/networking/routers/cisco-routers-ios.htm#Hardware%20Components)
[Cisco>Support>Product Support>End-of-Sale and End-of-Life Products>Cisco 3600 Series Multiservice Platforms>Troubleshoot and Alerts> Troubleshooting TechNotes> Understanding the 1-Port ISDN BRI \(S/T\) WAN Interface Card \(WIC-1B-S/T or WIC36-1B-S/T\)](#)

QUESTION 132

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 133

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 134

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 135

What port types are available for Rapid Spanning Tree Protocol (RSTP) but NOT available in Spanning Tree Protocol (STP)? (Choose two.)

- A. Root port
- B. Backup port
- C. Alternate port
- D. Designated port
- E. Learning port



Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

RSTP was developed to reduce the high convergence times required in STP, and introduces the alternate port and backup port roles. RSTP is an Institute of Electrical and Electronics Engineers (IEEE) standard, 802.1w, and is interoperable with 802.1d (STP). It operates on the Data Link layer of the OSI model.

An alternate port is a port that has an alternative path or paths to the root bridge, but is currently in a discarding state. A backup port is a port on a segment that could be used to reach the root port, but there is already an active designated port for the segment. An alternate port can also be described as a secondary, unused root port, and a backup port as a secondary, unused designated port.

A root port is a port on non-root switches used to reach the root switch. There can be only one root port on a switch, and it is determined by the least path cost to the root switch. Root ports are used in STP and RSTP.

A designated port is the port used by a network segment to reach the root switch. Designated ports lead away (downstream) from the root switch, and are determined by the lowest path cost to the root switch. While a switch can only have one root port, every other port could potentially be a designated port. Whenever a network segment could be serviced by more than one switch, STP will elect one switch as designated for the segment, and the other(s) will be

blocking. This is a core function of the STP protocol, in that only one active Layer 2 path can exist between any two network segments. This port type is available in STP.

A learning port is not a valid port type in STP or RSTP. Learning is one of the possible port states in STP and RSTP. STP has five port states; blocked, listening, learning, forwarding, and disabled. There are only three port states in RSTP; discarding, learning, and forwarding.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot STP-related optional features

References:

[Cisco > Technology Support > LAN Switching > Spanning Tree Protocol > Technology White Paper > Understanding Rapid Spanning Tree Protocol \(802.1w\)](#)

QUESTION 136

Which of the following is a classful routing protocol?

- A. RIPv1
- B. EIGRP
- C. BGPv4
- D. RIPv2



Correct Answer: A

Section: (none)

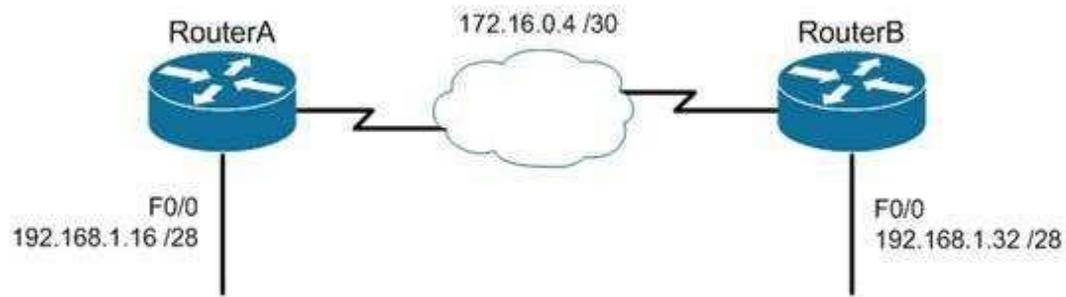
Explanation

Explanation/Reference:

Explanation:

The Routing Information Protocol version 1 (RIPv1) is a classful routing protocol, which exchanges routes without including any subnet masking information. IP addresses in the routing table should have the same subnet mask. Because classful routing protocols may not fully utilize the available IP address range, all router interfaces within the same network must have the same subnet mask.

Open Shortest Path First (OSPF), Routing Information Protocol version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol version 4 (BGPv4) are classless routing protocols. These protocols include the subnet mask in the route advertisement and support variable length subnet masks (VLSM). Intermediate System-to-Intermediate System (IS-IS) is also a classless routing protocol. An example of a network using VLSM is shown below. Note the different masks used, indicated with CIDR notation.



Objective: Routing
Fundamentals Sub-
Objective:

Compare and contrast distance vector and link-state routing protocols



References:

[Cisco > Articles > Cisco Networking Academy > CCNP 1: Advanced IP Addressing Management](#)
[Cisco > Internetworking Technology Handbook > Routing Information Protocol \(RIP\)](#)

QUESTION 137

You have the following configuration on your router:

```
ip dhcp pool POOLNAME network  
10.1.0.0 255.255.255.0  
default-router 10.1.0.254 dns-  
server 10.1.0.200
```

What command would you run to prevent the last available IP address in the scope from being allocated to a host via DHCP?

- A. ip dhcp restrict 10.1.0.254
- B. ip dhcp excluded-address 10.1.0.253

C. ip dhcp excluded-address 10.1.0.254

D. ip dhcp 10.1.0.253 excluded-address

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this scenario, you would run the ip dhcp excluded-address 10.1.0.253 command in global configuration mode to prevent DHCP allocation of the last available IP address in the scope. The ip dhcp excluded-address command is used to prevent DHCP from handing out IP addresses that are already statically configured on your network. The command can include a single IP address to exclude, or an entire range, such as:

```
Router(config)# ip dhcp excluded-address 10.1.0.100 10.1.0.125
```

The command above would block the entire range of 10.1.0.100 through 10.1.0.125 from being allocated by DHCP. If the next IP address in sequence to be assigned would have been 10.1.0.100, DHCP will skip the range and assign 10.1.0.126 as the next host address.

You would not execute ip dhcp excluded-address 10.1.0.254. This is the address of the router and it will automatically be excluded.

The other commands are incorrect because they are not valid Cisco IOS commands.

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 > Excluding IP Addresses](#)

QUESTION 138

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 unreachable 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 139

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-

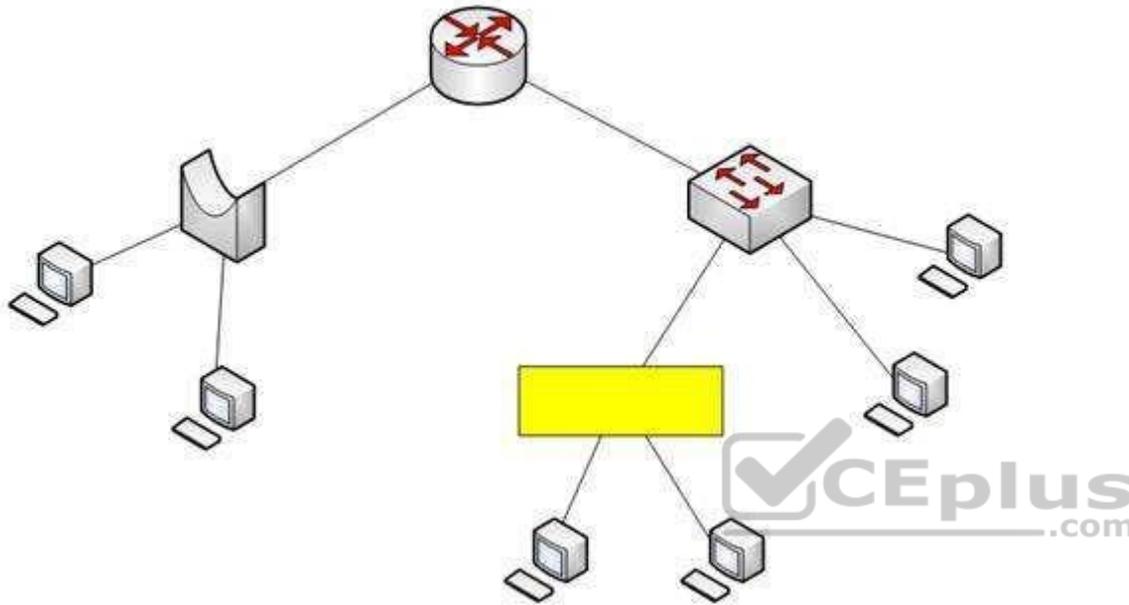
Objective:

Compare and contrast static routing and dynamic routing

References:

QUESTION 140

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 141

You wish to configure Secure Shell (SSH) support on your router so that incoming VTY connections are secure.

Which of the following commands must be configured? (Choose all that apply.)

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

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

The 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 142

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 143

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The no cdp run command is used to disable CDP on a Cisco router globally. CDP is a Layer 2 (Data Link layer) protocol that discovers information about neighboring network devices. CDP does not use network layer protocols to transmit information because it operates at the Data Link layer. Therefore, it is useful to determine information about directly connected Cisco network devices, because it can operate when network protocols have not been configured or are misconfigured. The show cdp neighbors detail command is used to view the IP addresses of the directly connected Cisco devices.

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

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

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

The disable cdp command is not a valid Cisco command.

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

References:
[Cisco > Cisco IOS Network Management Command Reference > show cdp neighbors](#)

QUESTION 144

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 145

You instructed your assistant to add a new router to the network. The routers in your network run OSPF. The existing router, OldRouter, is configured as follows:

```
router ospf 1 network 192.168.5.0
0.0.0.255 area 0 network 192.168.10.0
0.0.0.255 area 0
```

The OldRouter interface that connects to NewRouter is 192.168.5.3/24. Your assistant shows you the configuration that will be implemented:

```
newrouter(config)# router ospf 1 newrouter(config-router)#
network 192.168.5.0 255.255.255.0 area 0 What is wrong with this
configuration?
```

- A. The area ID is incorrectly configured.
- B. The wildcard mask is incorrectly configured.
- C. The network statement is incorrectly configured.
- D. The process ID number is incorrectly configured.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When entering network statements for OSPF, a wildcard mask is used instead of a regular mask. Since the network connecting the two routers is a class C network, as shown by the address 192.168.5.0/24, the wildcard mask should be 0.0.0.255 rather than 255.255.255.0. With wildcard masks, the 0s octets must match, and the 255s octets do not have to match.

The area ID is correct. OldRouter is in area 0, so NewRouter should be as well. There must be an area 0 in an OSPF network. There can be multiple areas as well, but they must all connect to area 0. If non-0 areas cannot be directly connected to area 0, they must be configured with a virtual link across an area that does connect to the backbone (area 0).

The network statement is correct. The network between the routers is 192.168.5.0.

The process ID number is correct. The number is stated as OSPF 1 on OldRouter and OSPF 1 on NewRouter. They match in this case but that is not required. Process IDs are only locally significant.

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:

[Internetworking Technology Handbook > Open Shortest Path First \(OSPF\)](#)



QUESTION 146

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 147

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 148

Which of the following is a Point-to-Point Protocol (PPP) authentication protocol that supports sending of hashed values instead of sending passwords in clear text?

- A. LCP
- B. NCP
- C. PAP
- D. CHAP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

There are two authentication methods available when implementing a PPP connection: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Challenge Handshake Authentication Protocol (CHAP) uses a one-way hash function based on the Message Digest 5 (MD5) hashing algorithm to hash the password. This hashed value is then sent across the wire. In this situation, the actual password is never sent. No one tapping the wire will be able to reverse the hash to come up with the original password. This is why MD5 is referred to as a one-way function. It cannot be reverse engineered. CHAP uses a three-way handshake process to perform the authentication. Moreover, CHAP periodically repeats the authentication process after link establishment.

When configuring PPP with CHAP authentication, both routers must be configured with a username that will be presented by the other router with a password. Therefore, the username to configure on Router A will be the username of Router B. The password should be the same on both machines. If these settings are not correct, then authentication will fail. The authentication process can be displayed as it happens with the debug PPP authentication command.

Link Control protocol (LCP) is defined in Request for Comments (RFCs) 1548 and 1570 and has primary responsibility to establish, configure, authenticate, and test a PPP connection. LCP negotiates the following when setting up a PPP connection:

- Authentication method used (PAP or CHAP), if any
- Compression algorithm used (Stacker or Predictor), if any
- Callback phone number to use, if defined
- Multilink; other physical connections to use, if configured

Network Control Protocol (NCP) defines the process for how the two PPP peers negotiate which network layer protocols, such as IP and IPX, will be used across the PPP connection. LCP is responsible for negotiating and maintaining a PPP connection whereas NCP is responsible for negotiating upper-layer protocols that will be carried across the PPP connection.

Password authentication Protocol (PAP) is simpler than CHAP, but less secure. During the authentication phase, PAP goes through a two-way handshake process. In this process, the source sends its user name (or hostname) and password in clear text, to the destination. The destination compares this information with a list of locally stored user names and passwords. If it finds a match, the destination returns an accept message. If it does not find a match, it returns a reject message.

Objective: WAN

Technologies Sub-

Objective:

Configure, verify, and troubleshoot PPPoE client-side interfaces using local authentication

References:

[Cisco > Internetworking Technology Handbook > Point-to-Point Protocol](#)

[Cisco > Support > Technology Support > WAN > Point-to-Point Protocol \(PPP\) > Design > Design TechNotes > Understanding and Configuring PPP CHAP Authentication > Document ID: 25647](#)

QUESTION 149

With which type of service is bandwidth and latency the biggest consideration?

- A. streaming video
- B. telnet sessions
- C. FTP transfers
- D. authentication traffic

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Streaming video places the largest demand on both bandwidth and latency. Video traffic is real-time and benefits from dedicated bandwidth with QoS implementation to ensure quality. Moreover, this service can tolerate very little latency.

Telnet and FTP sessions are both low bandwidth users and can tolerate a high degree of latency since the data can be reassembled when all pieces arrive, which is not possible when data is coming in real-time, and waiting for retransmissions and reassembly is not feasible.

Authentication traffic is not sensitive to latency and does not require much bandwidth either.

Objective: WAN

Technologies Sub-

Objective:

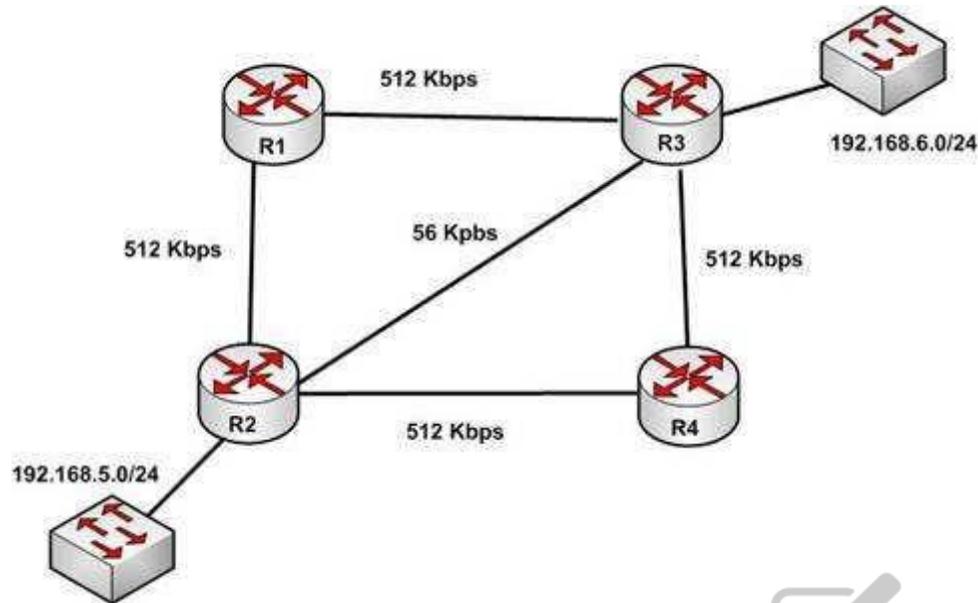
Describe basic QoS concepts

References:

[Cisco Documentation > Internetworking Technology Handbook > Voice/Data Integration Technologies](#)

QUESTION 150

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

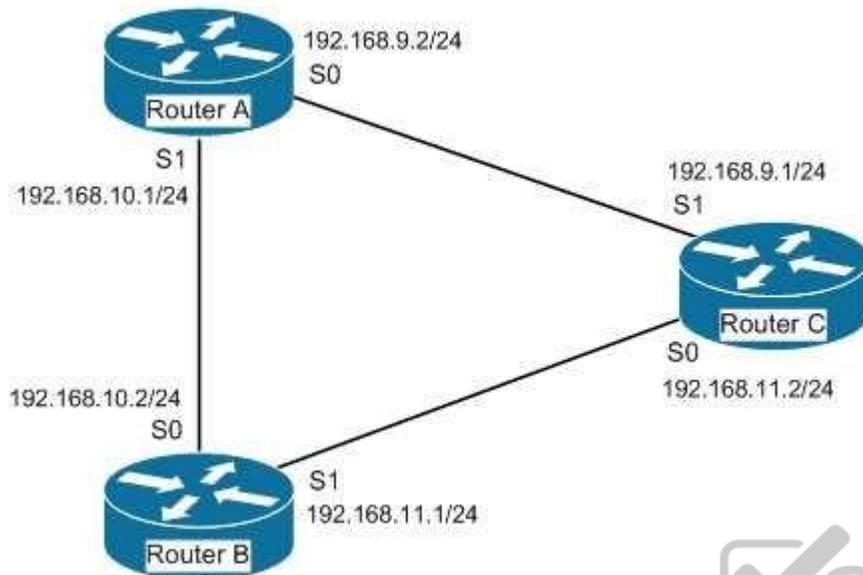
References:

[Home > Articles > Cisco Certification > CCDA > CCDA Self-Study: RIP, IGRP, and EIGRP Characteristics and Design](#)

QUESTION 151

You have three EIGRP routers that are connected as shown in the diagram below.





Router A and Router C do not seem to be exchanging information. You execute commands on all three routers, and receive as output the information shown below:

```
Router A# show ip eigrp neighbors
Address Interface holdtime uptime Q Seq SRTT RTO
192.168.10.2 S1 13 1:20:10 100 458 0 30
```

```
routerA# show run
<output omitted>
router eigrp 56
network 192.168.10.0
network 192.168.9.0
no auto-summary

routerC# show run
<output omitted>
router eigrp 56
network 192.168.11.0
no auto-summary
```

What needs to be done to make Routers A and C start exchanging information?

- A. Execute the auto-summary command on Router A

- B. Execute the network 192.168.9.0 command under EIGRP 56 on Router C
- C. Correct the IP address on the S1 interface of Router C
- D. Recreate the EIGRP configuration on Router C as EIGRP 55

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Router C is not displayed in the neighbor table of Router A, which indicates that Router C and Router A are not forming a neighbor relationship or exchanging information. This is because Router C does not have EIGRP configured for its S1 interface. You can see this is missing from its configuration in the output of the show run command for RouterC. To solve the issue, you should execute the network 192.168.9.0 command under the EIGRP 56 configuration on Router C. Then Router C will start sending hellos on that interface and the two routers will become neighbors.

The show ip eigrp neighbors command displays the following information for each EIGRP neighbor. In parentheses is the value of each found in the output of router A for Router B:

IP address (192.168.10.2)
Local interface (S1)
Retransmit interval (13)
Queue count (100)



There is no need to execute the auto-summary command on Router A. It will not affect the establishment of a neighbor relationship between Routers A and C.

There is no need to correct the IP address on the S1 interface of Router C. The address 192.168.9.1 is correctly located in the same subnet as the address on S0 of Router A.

Finally, changing the EIGRP configuration on Router C to EIGRP 55 will not help. Router C will not start sending hellos on its S1 interface until EIGRP is enabled on the S1 interface. Until then, the Routers A and C will not form a neighbor relationship and will not share information.

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 Configuration Guide, Release 12.4 > Configuring EIGRP > Enabling EIGRP](#)

QUESTION 152

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 153

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 154

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.
- Nonnegotiate: 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. Nonnegotiate mode enables trunking but disables DTP.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Configure and verify Layer 2 protocols



References:

QUESTION 155

Which command is NOT mandatory for inclusion in a plan to implement IP Service Level Agreements (SLAs) to monitor IP connections and traffic?

- A. ip sla
- B. ip sla schedule
- C. ip sla reset
- D. icmp-echo

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The ip sla reset command is not mandatory for an implementation plan to configure IP SLAs for monitoring IP connections and traffic. This command causes the IP SLA engine to either restart or shutdown. As a result, all IP SLAs operations are stopped, IP SLA configuration information is erased, and IP SLAs are restarted. The IP SLAs configuration information will need to be reloaded to the engine.

The following commands are essential to the implementation plan:

```
ip sla ip sla
schedule icmp-
echo
```

The ip sla command allows you to configure IP SLAs operations. When you execute this command in the global configuration mode, it enables the IP SLA configuration mode. In the IP SLA configuration mode, you can configure different IP SLA operations. You can configure up to 2000 operations for a given IP SLA ID number.

The icmp-echo command allows you to monitor IP connections and traffic on routers by creating an IP SLA ICMP Echo operation. This operation monitors end-to-end response times between routers.

The ip sla schedule command allows you to schedule the IP SLA operation that has been configured. With this command, you can specify when the operation starts, how long the operation runs, and how long the operation gathers information. For example, if you execute the ip sla schedule 40 start-time now life forever command, the IP SLA operation with the identification number 40 immediately starts running. This is because the now keyword is specified for the start-time parameter. Using the forever keyword with the life parameter indicates that the operation keeps collecting information indefinitely. Note that you cannot reconfigure the IP SLA operation after you have executed the ip sla schedule command.

The information gathered by an IP SLA operation is typically stored in RTTMON-MIB. A Management Information Base (MIB) is a database hosting information required for the management of routers or network devices. The RTTMON-MIB is a Cisco-defined MIB intended for Cisco IOS IP SLAs. RTTMON MIB acts as an interface between the Network Management System (NMS) applications and the Cisco IOS IP SLAs operations.

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](#)

[Cisco IOS IP SLAs Command Reference > icmp-echo through probe-packet priority > ip sla](#)

[Cisco IOS IP SLAs Command Reference > icmp-echo through probe-packet priority > ip sla schedule](#)

[Cisco > Cisco IOS IP SLAs Command Reference > icmp-echo](#)

QUESTION 156

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 servers 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 157

You execute the ping command from a host, but the router does not have a path to its destination.

Which of the following ICMP message types will a client receive from the router?

- A. ICMP redirect
- B. ICMP time exceeded
- C. ICMP destination unreachable
- D. ICMP echo-reply

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When a router receives a ping packet and has no route to the destination in its routing table, it will respond to the client with an ICMP destination-unreachable message. Internet Control Message Protocol (ICMP) is a Layer 3 protocol used to test the connectivity between hosts in a network. There are six types of unreachable destination message:

1. Network unreachable
2. Host unreachable
3. Protocol unreachable
4. Port unreachable
5. Fragmentation needed and Don't Fragment (DF) bit set
6. Source route failed

An ICMP redirect message would not be received. This type of response is received when the router is configured to direct clients to a different router for better routing.

An ICMP time-exceeded message would not be received. This type of response occurs when the router successfully sent the packet but did not receive an answer within the allotted time; in other words, the time-to-live of the ICMP packet has been exceeded.

An ICMP echo-reply message would not be received. This would be the response received if the destination received the ping command and responded successfully.

Objective:

Routing Fundamentals Sub-

Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

[Cisco > Internetworking Technology Handbook > Internet Protocols \(IP\) > Internet Control Message Protocol \(ICMP\)](#)

QUESTION 158

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(TOSO) 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 msec,
minimum inter SPF delay of 2000.000 msec,
maximum inter SPF delay of 4000.000 msec
Initial LSA generation delay 3000.000 msec,
```

```
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(TOSO) 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 msec,
minimum inter SPF delay of 2000.000 msec,
maximum inter SPF delay of 4000.000 msec
Initial LSA generation delay 3000.000 msec,
```



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 159

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 160

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 161

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

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

Explanation:

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

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

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

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

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

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

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

Configuration register is 0x2102

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

Router#configure terminal

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

Router(config)#config

Router(config)#config-register 0x2142

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

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

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

Objective:

Infrastructure Management Sub-

Objective:

Perform device maintenance



References:

[Cisco > Support > Routers > Cisco 10000 Series Routers > Troubleshoot and Alerts > Troubleshooting TechNotes > Use of the Configuration Register on All Cisco Routers > Document ID: 50421](#)

QUESTION 162

Which Cisco Internetwork Operating System (IOS) command can be used to configure the location of the configuration file?

- A. boot buffersize
- B. configure
- C. boot config
- D. service config

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The boot config command will configure the location of the configuration file. It must be followed by the copy run start command to be effective at next reboot. The syntax of the command is as follows:

boot config device:filename

The parameters of the command are as follows:

- Device : Specifies the device that contains the configuration file. ▪
- Filename : Specifies the name of the configuration file.

The boot buffersize command is incorrect because this command is used to modify the buffer size used to load the IOS image. Moreover, this command no longer functions in IOS 12.4.

The configure command is incorrect because this command is used to enter the global configuration mode.

The service config command is incorrect because this command is used to enable autoloading of configuration files from a network server.

Objective:

Infrastructure Management Sub-

Objective:

Perform device maintenance



References:

[Cisco > Cisco IOS Configuration Fundamentals Command Reference > A through B > boot config](#)

QUESTION 163

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 164

Which of the following are characteristics of Enhanced Interior Gateway Routing Protocol (EIGRP)? (Choose all that apply.)

- A. Requires a hierarchical physical topology
- B. Does not require a hierarchical physical topology
- C. Uses Diffusing Update Algorithm (DUAL) to provide loop prevention
- D. Uses Bellman-Ford algorithm to provide loop prevention
- E. Supports Message-Digest Algorithm 5 (MD5) authentication

- F. Does not support Message-Digest Algorithm 5 (MD5) authentication
- G. Can differentiate between internal and external routes
- H. Uses a 32-bit metric

Correct Answer: BCEGH

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EIGRP does not require a hierarchical physical topology. It uses Diffusing Update Algorithm (DUAL) to provide loop prevention, and it supports Message-Digest Algorithm 5 (MD5) authentication. It can differentiate between internal and external routes, and uses a 32-bit metric.

EIGRP is a classless protocol that allows the use of variable length subnet masks (VLSM) and supports classless interdomain routing (CIDR) for allocation of IP addresses. The following are characteristics of EIGRP:

- Supports large networks due to high scalability
- Provides fast convergence using the Diffusing Update Algorithm (DUAL)
- Performs equal and unequal load balancing by default
- Supports variable length subnet masks (VLSM) and classless interdomain routing (CIDR)
- Is a hybrid routing protocol (distance-vector protocol) that also provides link-state protocol characteristics

Is a classless protocol

- Sends partial route updates only when there are changes, reducing bandwidth usage for routing updates
- Has an administrative distance of 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes
- Is used only with Cisco platforms
- Provides support for IP IPX and AppleTalk protocols
- Can differentiate between internal and external routes
- Uses a 32-bit metric

EIGRP can load-balance up to four unequal cost paths. To do so, use the variance n command to instruct the router to include routes with a metric of less than n times the minimum metric route for that destination. The variable n can take a value between 1 and 128. The default is 1, which means equal cost load balancing.

The option stating that EIGRP requires a hierarchical physical topology is incorrect because EIGRP does not require or support a hierarchical routing topology.

The option stating that EIGRP uses Bellman-Ford algorithm to provide loop prevention is incorrect. EIGRP uses DUAL to provide loop prevention.

Objective:

Routing Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

[Cisco > Internetworking Technology Handbook > Enhanced Interior Gateway Routing Protocol \(EIGRP\)](#)

QUESTION 165

You have implemented SNMP v3 in your network. After making the configuration changes, you find that technicians in the TECHS group cannot access the MIB. You execute the show run command and receive the following output that relates to SNMP:

```
<output omitted>

snmp-server group NORMAL v3 priv read NORMAL write NORMAL
snmp-server group TECHS v3 priv read TECHS access 99
snmp-server group TRAP v3 priv

!!
snmp-server user NORMAL NORMAL v3 auth sha CISCO priv des56 CISCO
snmp-server user TECHS TECHS v3 auth sha CISCO priv des56 CISCO
snmp-server user TRAP TRAP v3 auth sha CISCO priv des56 CISCO

snmp-server enable traps snmp linkup linkdown
snmp-server host 155.1.146.100 traps version 3 priv TRAP
```

What is preventing the TECHS group from viewing the MIB?

- A. The presence of the keyword priv in the command creating the RESTRICTED group
- B. A mismatch between the authentication mechanism and the encryption type in the command creating the TECHS user
- C. The absence of an access list defining the stations that can be used by the TECHS group
- D. The presence of the keyword auth in the command creating the TECHS user

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The command that creates the TECHS group ends with the parameter access 99: snmp-

```
server group TECHS v3 priv read TECHS access 99
```

This indicates that the access list number 99 is specifying the IP addresses of the stations allowed to connect to the MIB for the group. Since the access list is missing from the configuration, no IP addresses will be allowed, and no connections can be made by the group.

The presence of the keyword `priv` in the command creating the `TECHS` group is not causing the issue. This keyword indicates that encryption (privacy) and authentication should both be used on all transmissions by the group.

In `SNMPv3`, 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

There is no mismatch between the authentication mechanism and the encryption type in the command creating the `TECHS` user.

```
snmp-server user TECHS TECHS v3 auth sha CISCO priv des56 CISCO
```

In the preceding command, the section `auth sha CISCO` specified that messages are authenticated using SHA with a key of `CISCO`. It does not need to match the section `priv des56 CISCO`, which indicates that encryption (`priv`) will be provided using DES56 with a key of `CISCO`.

The presence of the keyword `auth` in the command creating the `TECHS` user is not causing the issue. This line indicates that that messages are authenticated using SHA with a key of `CISCO`.



Objective:

Infrastructure Management Sub-

Objective:

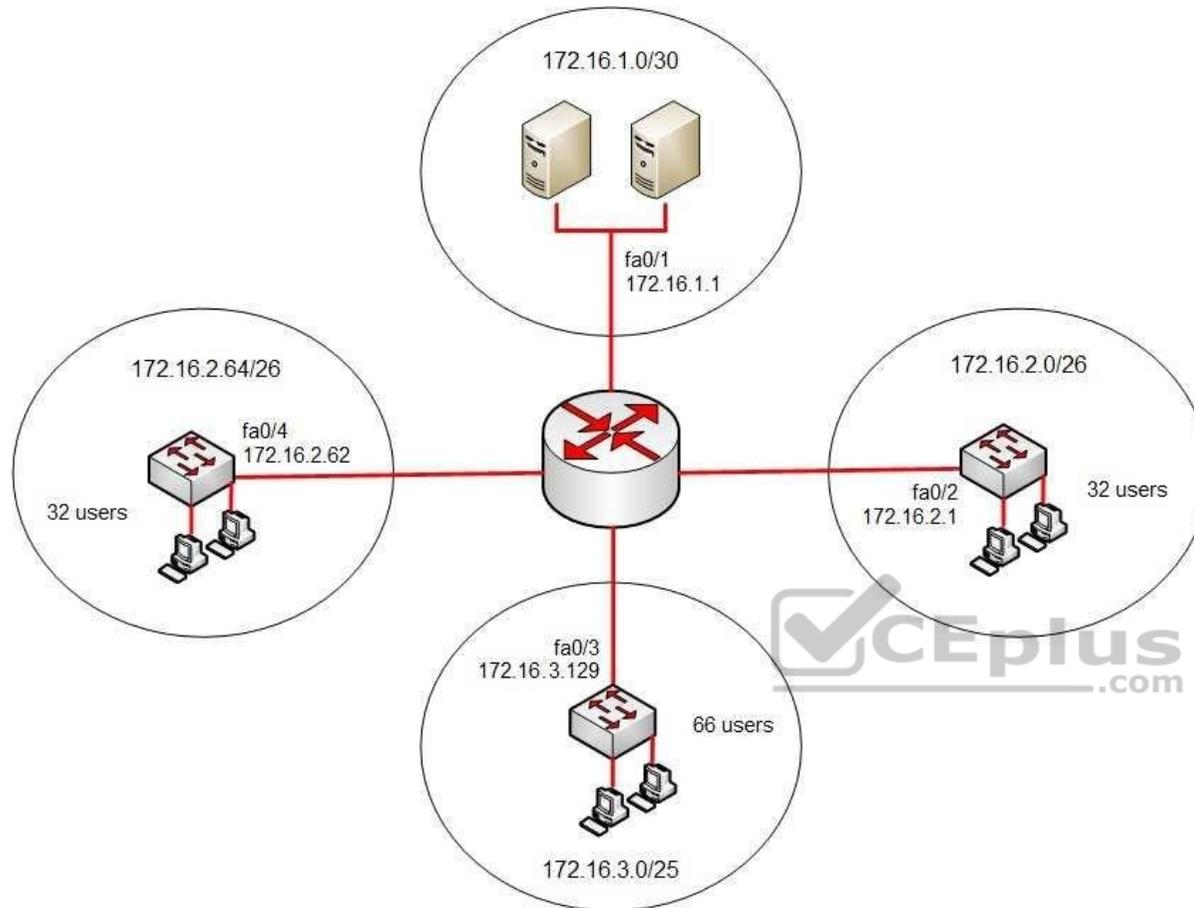
Configure and verify device-monitoring protocols

References:

[SNMP Configuration Guide, Cisco IOS XE Release 3SE \(Catalyst 3850 Switches\) > SNMPv3](#)

QUESTION 166

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:

$$2^n - 2 = X$$

(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
172.16.0.128
172.16.1.0
172.16.1.128
172.16.2.0
172.16.2.128
172.16.3.0
172.16.3.128

...and so on, incrementing each time by 128 in the last octet

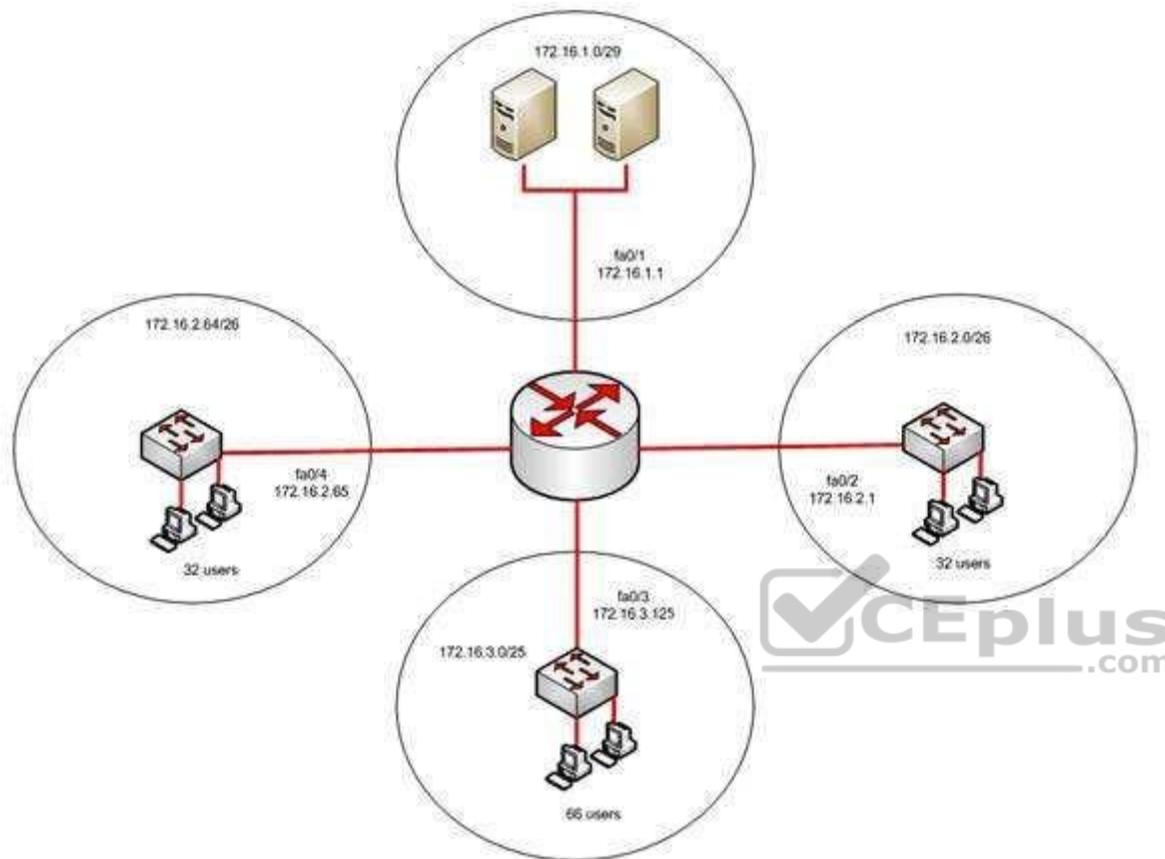
Interface Fa0/3 should be allocated an IP address in the 172.16.3.1 through 172.16.3.126 range.

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 172.16.2.65-172.16.2.126. 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 167

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.

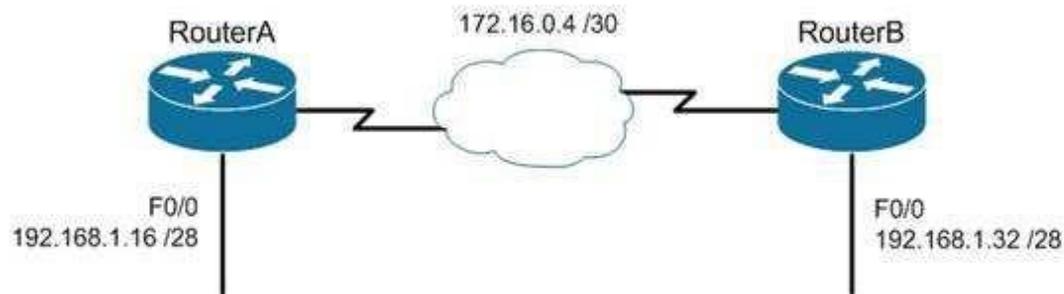
Intermediate-System-to-Intermediate System (IS-IS) is also a classless routing protocol.

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 discontinuous networks. When subnets of the same classful network are separated by another classful network, the networks are called discontinuous. 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 168

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 169

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 170

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 171

Which of the following are Wide Area Network (WAN) protocols? (Choose three.)

- A. PPP
- B. AAA
- C. WEP
- D. STP
- E. HDLC
- F. Frame Relay

Correct Answer: AEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), and Frame Relay are WAN protocols.

PPP is a WAN protocol is defined in Request for Comments (RFCs) 1332, 1661, and 2153. PPP works with asynchronous and synchronous serial interfaces as well as High-Speed Serial Interfaces (HSSI) and Integrated Services Digital Network (ISDN) interfaces (BRI and PRI). Some of the characteristics of PPP are:

- Can be used over analog circuits
- Can encapsulate several routed protocols, such as TCP/IP
- Provides error correction
- Should be used rather than HDLC when non-Cisco routers are involved, as it is implemented consistently among vendors ▪

PPP authentication can be used between the routers to prevent unauthorized callers from establishing an ISDN circuit

To change the encapsulation from the default of HDLC to PPP when connecting to a non-Cisco router, such as a Juniper, you would use the following command:

```
router(config)#interface serial S0 router(config-  
if)#encapsulation ppp
```



HDLC is a WAN protocol used with synchronous and asynchronous connections. It defines the frame type and interaction between two devices at the Data Link layer.

Frame Relay is a group of WAN protocols, including those from International Telecommunication Union (ITU-T) and American National Standards Institute (ANSI). Frame Relay defines interaction between the Frame Relay customer premises equipment (CPE) and the Frame Relay carrier switch. The connection across the carrier's network is not defined by the Frame Relay standards. Most carriers, however, use Asynchronous Transfer Mode (ATM) as a transport to move Frame Relay frames between different sites.

Authentication, Authorization, and Accounting (AAA) is incorrect because this is a scheme to monitor access control and activities on networked devices.

Wired Equivalent Privacy (WEP) is a security scheme for wireless networks and therefore it is incorrect.

Spanning Tree Protocol (STP) is for loop avoidance in redundant topologies. This option is incorrect because this protocol is used on Local Area Network (LAN).

Objective: WAN

Technologies Sub-

Objective:

Describe WAN access connectivity options

References:

[Cisco > Internetworking Technology Handbook > Point-to-Point Protocol](#)

[Cisco > Internetworking Technology Handbook > Frame Relay](#)

[Cisco > Support > Technology Support > WAN > High-Level Data Link Control \(HDLC\) > Configure > Configuration Examples and TechNotes > HDLC Back-to-Back Connections > Document ID: 7927](#)

QUESTION 172

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 173

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 174

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 175

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 network's 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 176

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 output 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 177

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

Which deployment model should be implemented to accomplish the task?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

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

Objective:

Network Fundamentals Sub-

Objective:

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

References:

[Cisco > Dual Stack Network](#)

[Cisco > Technology Support > IP > IPv6 > Configure > Configuration Examples and TechNotes > Tunneling IPv6 through an IPv4 Network > Document ID: 25156](#)

QUESTION 178

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 179

Which is the valid IP address range that can be assigned to hosts on the subnet that includes the address 172.16.4.6/23?

- A. 172.16.2.1 - 172.16.4.254
- B. 172.16.3.1 - 172.16.5.254
- C. 172.16.4.1 - 172.16.5.254
- D. 172.16.4.1 - 172.16.4.254

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

172.16.4.1 - 172.16.5.254 is the valid IP address range that can be assigned to hosts on the subnet that includes the address 172.16.4.6/23.

To determine the range of addresses that can be assigned in a subnet, you must first determine the network ID and broadcast address of the subnetwork. All addresses that can be assigned to hosts will lie between these two endpoints. The network ID can be obtained by determining the interval between subnet IDs. With a 23-bit mask, the decimal equivalent of the mask will be 255.255.254.0. 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 - 254. Therefore, the interval is 2, and it is applied in the third octet where the subnet mask ends.

The first network ID will always be the classful network you started with (in this case 172.16.0.0). Then each subnetwork ID will fall at 16-bit intervals as follows:

172.16.0.0

172.16.2.0

172.16.4.0

172.16.6.0

At 172.16.6.0 we can stop because the address that we are given in the scenario, 172.16.4.6, is in the network with a subnet ID of 172.16.4.0. Therefore, since the broadcast address for this network will be 1 less than the next subnet ID, or 172.16.5.255, the valid range is 172.16.4.1 - 172.16.5.254.

All the other options are incorrect because these are not valid IP address ranges for this scenario.

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 180

You are working with an Internet Service Provider (ISP) as network manager. A corporate client approaches you to lease a public IP subnet that can accommodate 250 users. You have assigned him the 192.25.27.0 subnet.

What subnet mask should be assigned to this IP address so that it can accommodate the number of users required by the corporate client?

- A. 255.255.255.0
- B. 255.255.255.128
- C. 255.255.255.224
- D. 255.255.255.252



Correct Answer: A

Section: (none)

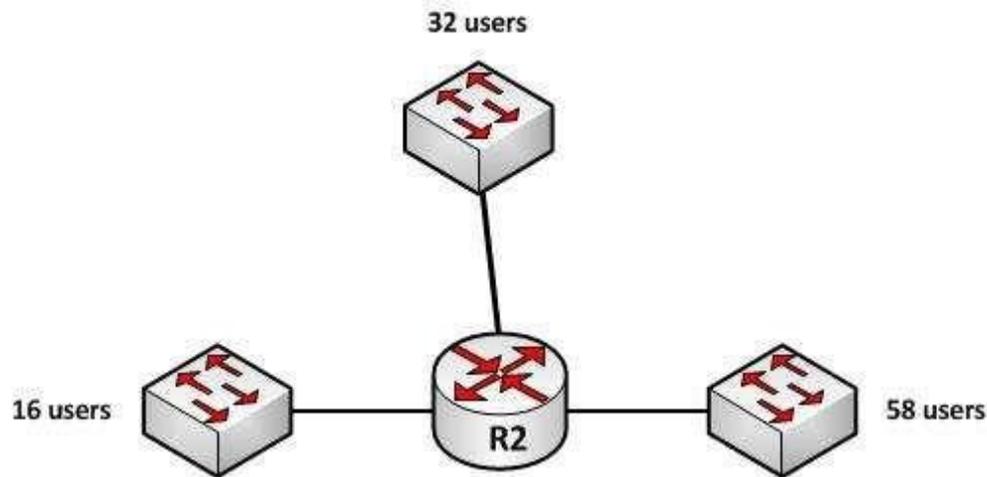
Explanation

Explanation/Reference:

Explanation:

The 192.25.27.0 subnet should be assigned the subnet mask of 255.255.255.0 to accommodate 250 users. This subnet mask can accommodate a maximum of 254 hosts. The number of hosts that can reside on a subnet can be calculated using the formula $2^n - 2 = x$, where n is equal to the number of hosts bits in the mask and x is the resulting number of hosts. 2 is subtracted from the results to represent the two addresses, the network ID and the broadcast address, that cannot be assigned to computers in the subnet. Since the 255.255.255.0 mask leaves 8 bits at the end of the mask, the formula will be $2^8 - 2$, which is $256 - 2$, which equals 254.

In situations where the same subnet mask must be used for multiple interfaces on a router, the subnet mask that is chosen must provide capacity sufficient for the largest number of hosts on any single interface while also providing the required number of subnets. For example, in the diagram below, the three interfaces on the router R2 have 16, 32 and 58 users respectively on each interface:



If each interface must have the same subnet mask, the subnet mask would need to be one that yields at least 58 addresses to support the interface with the highest host count and yields at least 3 subnets as well.

If the chosen classful networks were 128.107.4.0/24, the correct mask would be 255.255.255.192. Since the mask is currently 255.255.255.0 (/24), by borrowing 2 bits to /26 or 255.255.255.192, we will get 4 subnets ($2^2 = 4$) and each subnet will yield 62 hosts ($2^6 - 2 = 62$).

With a subnet mask of 255.255.255.128, the 192.25.27.0 subnet can accommodate only 126 hosts. The mask 255.255.255.128 leaves 7 host bits in the mask and when we plug that into the formula we get $2^7 - 2$, which equals 126.

With a subnet mask of 255.255.255.224, the 192.25.27.0 subnet can accommodate only 30 hosts. The mask 255.255.255.224 leaves 5 host bits in the mask and when we plug that into the formula we get $2^5 - 2$, which equals 30.

With a subnet mask of 255.255.255.252, the IP address 192.25.27.24 can accommodate only two hosts. The mask 255.255.255.252 leaves 2 host bits in the mask and when we plug that into the formula we get $2^2 - 2$, which equals 2.

Objective:

Network Fundamentals Sub-

Objective:

Apply troubleshooting methodologies to resolve problems

References:

[Cisco > Design Tech Notes > IP Routing > IP Addressing and Subnetting for New Users > Understanding IP Addresses > Document ID: 13788](#)

QUESTION 181

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 182

Which Internet Control Message Protocol (ICMP) message is sent by a host in the network to test connectivity with another host?

- A. ICMP redirect message
- B. ICMP echo-request message
- C. ICMP time-exceeded message
- D. ICMP destination-unreachable message

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An ICMP echo-request message is sent by a host in the network to test connectivity with another host. An ICMP echo-request message is generated by the ping command. ICMP is a network-layer protocol that uses packets for reporting informational messages. When a host receives an echo-request (a ping), it responds by sending back an echo-reply message.

An ICMP redirect message is sent to the source host by the router to make the routing process more efficient.

An ICMP time-exceeded message indicates that the Time-to-Live (TTL) field of the IP packet has reached zero.

An ICMP destination-unreachable message is sent by the router to indicate that the router is unable to send the packet to its intended destination.

Objective:

Network Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

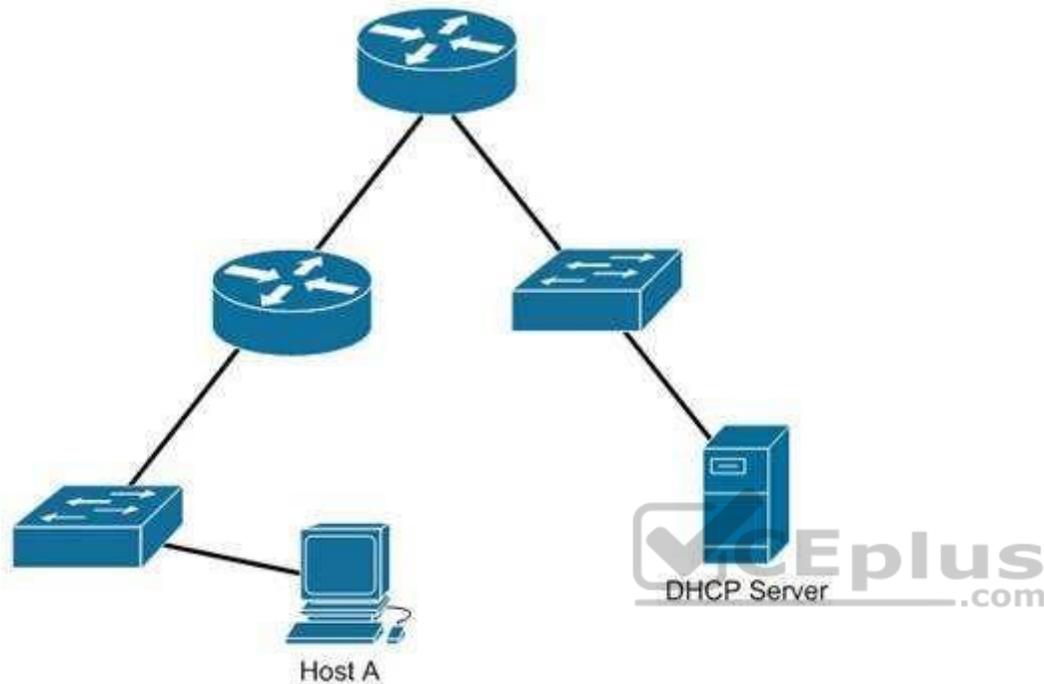
References:

[Cisco > Internetworking Technology Handbook > Internet Protocols \(IP\)](#)

QUESTION 183

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 184

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Switchport security can be used to:

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

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

Objective:

Infrastructure Security Sub-

Objective:

Configure, verify, and troubleshoot port security

References:

[Cisco > Catalyst 2950 and Catalyst 2955 Switch Command Reference, 12.1\(22\)EA11 and Later > Catalyst 2950 and 2955 Switch Cisco IOS Commands - s > switchport port-security](#)

QUESTION 185

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 186

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 187

Which of the following is NOT true of APIC-EM?

- A. It supports greenfield but not brownfield deployments
- B. It provides a single point for network automation
- C. It saves time and cost
- D. It is open and programmable

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Cisco Application Policy Infrastructure Controller Enterprise Module (APIC_EM) is an SDN controller platform that supports both greenfield implementations, which use no previous code and design from the ground up, and brownfield implementations, which incorporate existing code.

APIC-EM does provide a single point for network automation. This automation leads to both time and cost savings.

APIC-EM uses an open and programmable approach to devices, policies, and analytics.

Objective:

Infrastructure Security Sub-

Objective:

Verify ACLs using the APIC-EM Path Trace ACL analysis tool

References:

QUESTION 188

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 189

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 190

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, Cisc0\$ell\$, 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 191

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 sicso
```



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 192

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 193

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 194

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 195

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.

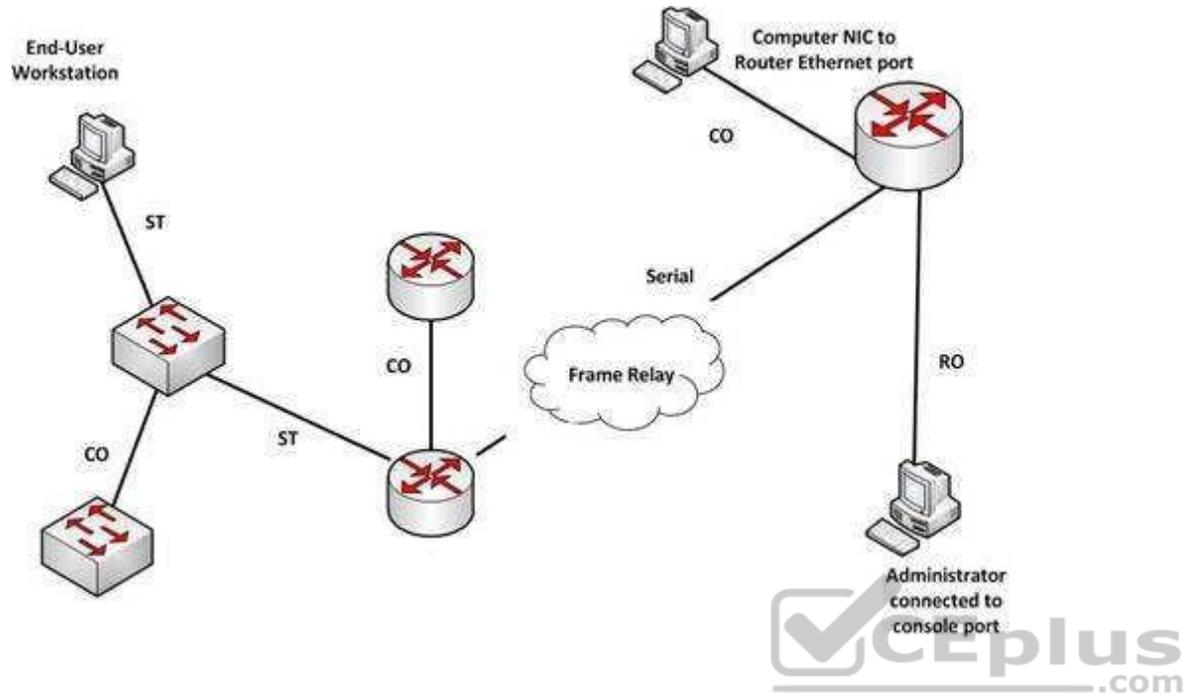
The diagram below illustrates the correct usage of each of the cable types shown using the following legend: ▪

SO Ethernet Straight through Cable

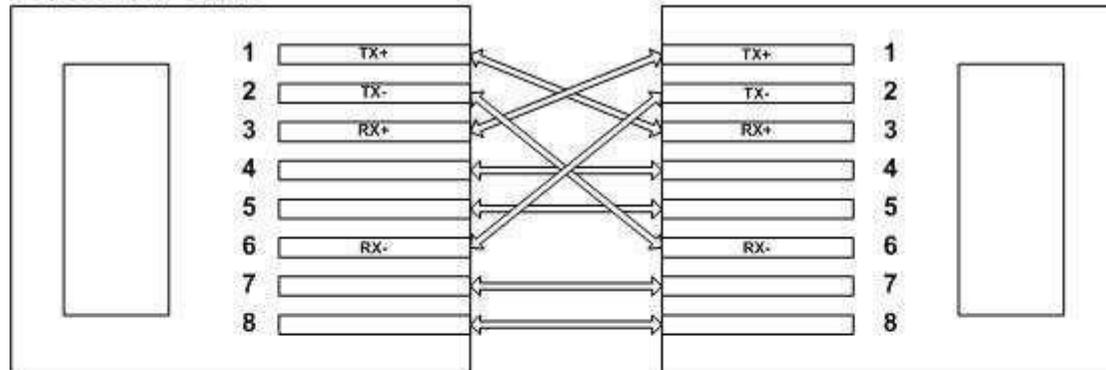
▪ CO Ethernet Crossover Cable ▪

Serial Serial cable

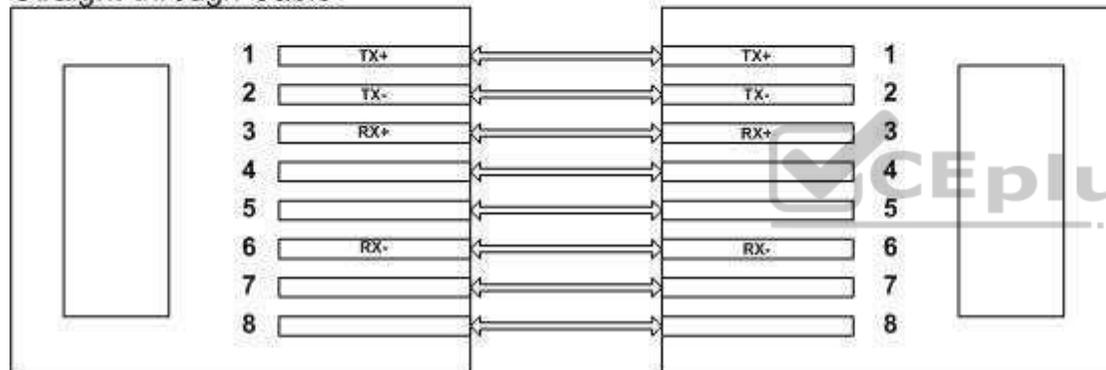
▪ RO Rollover cable



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 196

You are implementing IP SLA and would like to use it to measure hop-by-hop response time between a Cisco router and any IP device on the network.

Which of the following IP SLA operations would you use for this?

- A. ICMP path echo operation
- B. Internet Control Message Protocol Echo Operation
- C. UDP Jitter Operation for VoIP
- D. UDP Jitter Operation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The ICMP path echo operation discovers the path using the traceroute command, and then measures response time between the source router and each intermittent hop in the path. IP SLAs allow users to monitor network performance between Cisco routers or from a Cisco router to a remote IP device.

The Internet Control Message Protocol (ICMP) Echo Operation measures end-to-end response time between a Cisco router and any IP-enabled device. Response time is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. It does not measure hop-by-hop response time.

The UDP Jitter Operation for VoIP is an extension to the current jitter operations with specific enhancements for VoIP. The enhancements allow this operation to calculate voice quality scores and simulate the codec's directly in CLI and the MIB. It does not measure hop-by-hop response time.

The UDP Jitter Operation is designed to measure the delay, delay variance, and packet loss in IP networks by generating active UDP traffic. It does not measure hop-by-hop response time.

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 197

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 $100,000,000/\text{bandwidth}$. 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 equal-cost 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 198

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 199

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, serial10/0
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 200

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 201

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 202

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.)



<https://vceplus.com/>

- 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 203

You are troubleshooting a problem with two routers configured in a HSRP group. You intended to configure the routers so that Router A and Router B would each track their respective Fa0/1 interfaces and decrement their priorities for several VLAN groups if the tracked interface went down. However, you find that Router A is not taking over as the active device for the HSRP group on VLAN 101 when the Fa0/1 interface on Router B fails.

Which command would NOT be useful for discovering the problem?

- A. show running-configuration
- B. show vlans
- C. show standby brief

D. show standby

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show vlans command would NOT be useful for discovering the problem. When troubleshooting a problem with Hot Standby Router Protocol (HSRP), the show vlans command will yield no useful information. The output of the command is shown below, demonstrating that there is no HSRP information provided.

```
router# show vlan trunk
VLAN Name          Status      IfIndex Mod/Ports, Vlans
-----
1      default      active      5      2/1-26/4-8
15     VLAN0015     active      18     6/1,6/3
16     VLAN0016     active      19     6/2
23     VLAN0023     active      20
26     VLAN0026     active      21
31     VLAN0031     active      22
39     VLAN0039     active      23
```



All three of the remaining commands will be useful in discovering information. Each is shown below with an example of its application to troubleshooting.

Example A: show running-configuration

Router B is not taking over as the active device for VLAN 101's HSRP group when the Fa0/1 interface on Router A fails. Below is a partial output of show run for both routers with the output focused on the section concerning VLAN 101's configuration on each.

The above output displays the source of the problem. Router A has a decrement value of 5 configured for Fa0/1, as shown on the last line of the output after the specification of Fastethernet 0/1. This means that when its Fa0/1 interface goes down, Router A will subtract 5 from its priority for the VLAN 101 group, lowering it to 175. This is still higher than the priority of Router B, which is 170. Therefore, the solution is to change the decrement value for Router A to at least 11. When the interface goes down, Router A's priority will be decremented to 169, allowing Router B to take the role as active for the HSRP group in VLAN 101.

Example B: show standby brief

Router C is not taking over as the active device for VLAN 102's HSRP group when the Fa0/1 interface on Router D fails. Below is a partial output of show standby brief for both routers C and D, with the output focused on the section concerning VLAN 102's configuration on each.

Router C

```
Interface Grp Prio P State Active addr Standby addr Group addr
Fa0/1 102 200 Active local 10.10.10.253 10.10.10.251
```

Router D

```
Interface Grp Prio P State Active addr Standby addr Group addr
Fa0/1 102 200 P Active local 10.10.10.253 10.10.10.251
```

The absence of a P in the P (preempt) column in the output for Router C shows that it is not set to preempt. If not configured to preempt, it will never take over for Router D, regardless of its priority with respect to Router D.

Example C: **show standby**

Router F is supposed to be the active router for VLAN 103's HSRP group. Occasionally both routers are shut down for maintenance over the weekend. After the routers are rebooted, Router F is not taking over as the active device for VLAN 103's HSRP group. Below is a partial output of the show standby command for both routers, with the output focused on the section concerning VLAN 103's configuration on each



Router E

```
Fastethernet 0/1 - Group 1
State is Active
2 state changes, last state change 00:30:59
Virtual IP address is 10.1.0.20
Secondary virtual IP address 10.1.0.21
Active virtual MAC address is 0004.4d82.7981
Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is local
Standby router is 10.1.0.7, priority 140(expires in 9.184 sec)
Priority 200 (configured 200)
Tracking interface Fastethernet 0/1 state up decrement 10
```

Router F

```
Fastethernet 0/1 - Group 1
State is Active
2 state changes, last state change 00:30:59
Virtual IP address is 10.1.0.20
Secondary virtual IP address 10.1.0.21
Active virtual MAC address is 0004.4d82.7981
Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is 10.1.0.6, priority 190(expires in 9.184 sec)
Standby router is local
Priority 190 (configured 190)
Tracking interface Fastethernet 0/1 state up decrement 50
```



The output shows that Router F is not assuming the active role because of the priority and decrement values configured on the routers. When both routers go down, Router E will decrement its priority (200) by 10, as shown in last two lines of its output, leaving the priority at 190. Router F will decrement its priority (190) by 50 as shown in last two lines of its output, leaving the priority at 140. Therefore, to ensure that Router F maintains its role as active even after the dual shutdowns,

the priority of Router F should be increased to at least 241. When both routers decrement their priorities after shutdown, Router F will then have a priority of 191, which will be higher than the priority value of Router E.

Objective:

Infrastructure Services Sub-

Objective:

Configure, verify, and troubleshoot basic HSRP

References:

[Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks](#)

[Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands](#)

QUESTION 204

You set up several routers in your lab. Two of them are connected back to back using Data Terminal Equipment (DTE)-to-Data Circuit-terminating Equipment (DCE) cable. You need to configure the clock rate.

On which router would you configure the clock rate?

- A. the DCE
- B. the DTE
- C. The clock rate is set by default
- D. The clock rate cannot be configured



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The clock rate is set on the Data Circuit-terminating Equipment (DCE) device. DCE is also known as Data Communications Equipment.

DCE terminates a physical WAN connection and provides clocking and synchronization of a connection between two locations and connects to a DTE. The DCE category includes equipment such as CSU/DSUs and modems. If you were connecting a router to a WAN link, the router would be the DTE end and would be connected to a CSU/DSU or a modem. Either of these devices would provide the clocking.

DTE is an end-user device, such as a router or a PC that connects to the WAN via the DCE device.

Other options are incorrect. By default, no clock rate is configured, but can be set on a DCE device by using the clock rate [bps] command.

Objective:

WAN Technologies Sub-

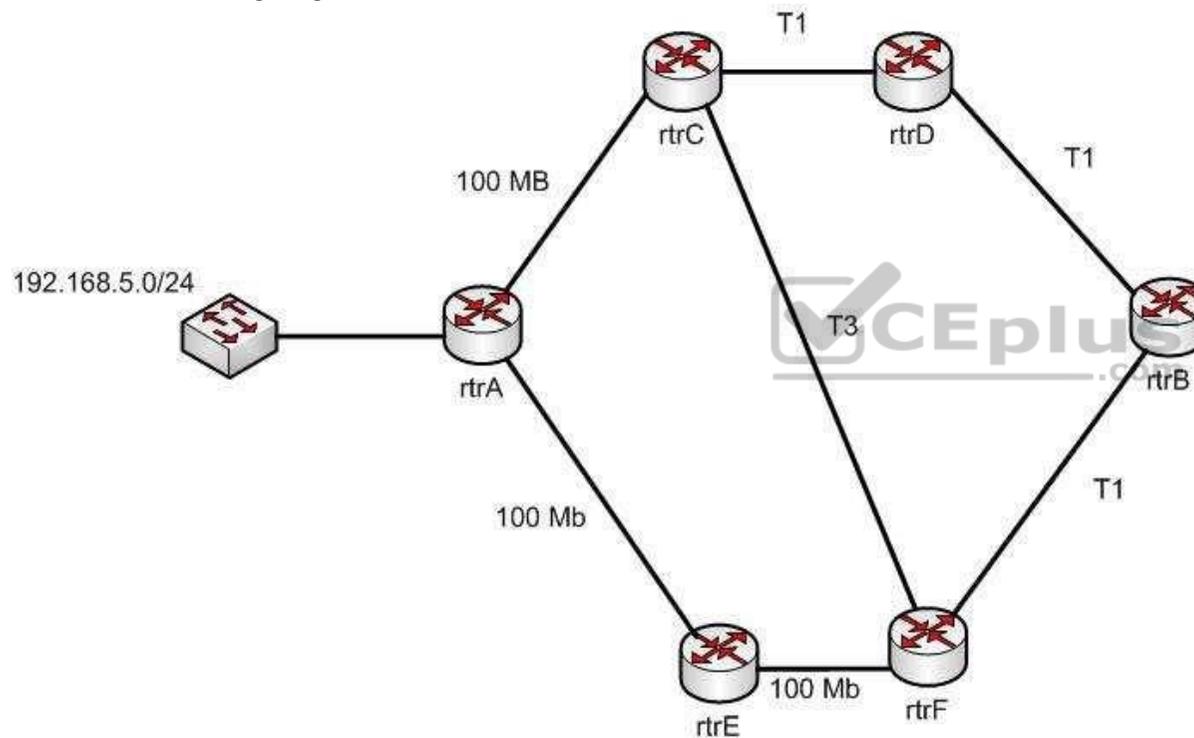
Objective:

Describe WAN access connectivity options

References:

QUESTION 205

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:

[Home > Support > Technology Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > OSPF Cost](#)

QUESTION 206

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 207

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 208

The execution of the show interfaces command yields the following as a part of its output:

```
Ethernet 0/0 is up, line protocol is down
```

Which of the following can be determined from this output?

- A. the link is not functional due to a Data Link layer issue
- B. the link is fully functional
- C. the link is not functional due to a Physical layer issue
- D. the link is not functional due to both a Physical layer and a Data Link layer issue



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The command output excerpt indicates that the link is not functional due to a Data Link layer (or "line protocol") issue, while the Physical layer (Layer 1) is operational. The first (left) column indicates the Physical layer state of the interface, while the second (right) column indicates the Data Link layer state of the interface.

The link is not fully functional. Were it fully functional, the command output would be:

```
Ethernet0/0 is up, line protocol is up
```

The link is not suffering a Physical layer issue or a combination of Physical layer and Layer 2 (Data Link) layer issues. Were either the case, the output would be:

```
Ethernet 0/0 is down, line protocol is down
```

Note: if a Physical layer issue exists, there will also be a Data Link issue, since the Data Link layer depends on the Physical layer to provide connectivity.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

[Cisco > Support > Cisco IOS Interface and Hardware Component Command Reference > show interfaces](#)

QUESTION 209

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
Typing 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 210

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 211

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 212

Which device will always have all of its ports in the same collision domain?

- A. Hub
- B. Bridge
- C. Switch
- D. Router

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Open Systems Interconnect (OSI) Layer 1 devices, such as hubs and repeaters, do not create multiple collision domains. All of their ports remain in the same collision domain as well as the same broadcast domain.

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. Replacing a hub with a switch effectively eliminates collisions for devices connected to the switch ports.

Bridges and switches create multiple collision domains and can reduce collisions within a broadcast domain, as each port constitutes a separate collision domain. However, if the network is not segmented with Virtual LANs (VLANs), all ports remain in the same broadcast domain. The main difference between a bridge and a switch is that the latter has a higher port capacity and better performance. VLANs segment the network into smaller broadcast domains using a Layer 2 device such as switch.

Routers segment the network into multiple broadcast domains. Routers are Layer 3 devices, and thus they interconnect different Layer 3 IP networks. Every interface/subinterface on a router has a unique IP network/subnet address that corresponds to a broadcast domain. Thus, every interface on a router defines a broadcast domain.

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

References:
[Cisco > Internetworking Technology Handbook > Routing Basics](#)

QUESTION 213

Which of the following commands will configure a router to use DNS for hostname resolution?

- A. ip dns primary
- B. ip domain lookup
- C. ip dns server
- D. ip name-server

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The ip domain lookup command configures the device to use DNS for hostname resolution. It must be accompanied by a command that specifies the location of the DNS server, which is done with the ip name-server command.

The ip dns-primary command is used to configure the device as the primary DNS name server for a domain (zone) and as the start of authority (SOA) record source, which designates the start of a zone.

The ip dns server command is used to make the device a DNS server.

Objective:
Infrastructure Services Sub-
Objective:
Describe DNS lookup operation

References:
[Home > Support > IP Addressing: DNS Configuration Guide, Cisco IOS Release 15M&T](#)

QUESTION 214

Which Cisco Internetwork Operating System (IOS) command is used to view information about the Dynamic Host Configuration Protocol (DHCP) address pool?

- A. show ip dhcp server statistics
- B. show ip dhcp pool
- C. show dhcp pool
- D. show ip dhcp server pool

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show ip dhcp pool command is used to view information about the DHCP address pool. The following code is a sample output of this command:

```
Pool 1:
Utilization mark (high/low) : 105 / 23
Subnet size (first/next) : 24 / 24 (autogrow)
VRF name : abc
Total addresses : 55
Leased addresses : 24
Pending event : none
3 subnets are currently in the pool :
Current index IP address range Leased addresses
25.1.1.12 25.1.1.1 - 25.1.1.14 11
25.1.1.17 25.1.1.17 - 25.1.1.30 0
Interface Ethernet0/1 address assignment
25.1.1.1 255.255.255.248
25.1.1.17 255.255.255.248 secondary
```



The show ip dhcp server statistics command is incorrect because this command is used to view the statistics of the DHCP server.

The show dhcp pool command and show ip dhcp server pool commands are both incorrect because these are not valid Cisco IOS commands.

Objective:

Infrastructure Services Sub-

Objective:

Troubleshoot client- and router-based DHCP connectivity issues

References:

QUESTION 215

Which two statements are TRUE of Internet Protocol (IP) addressing? (Choose two.)

- A. Public addresses are registered with the Internet Assigned Numbers Authority (IANA).
- B. These addresses are publicly registered with the Internet Service Provider (ISP).
- C. Through a public IP address, you can access another computer on the Internet, such as a Web server.
- D. The ranges of public IP addressing are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.
- E. Private addresses are allocated by the Internet Assigned Numbers Authority (IANA).

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Public addresses are publicly registered with the Internet Assigned Numbers Authority (IANA). Through a public IP address, you can access an Internet computer like a Web server.

The following statements are true of public IP addressing:

- These addresses are publicly registered with the Internet Assigned Numbers Authority (IANA)
- Through a public IP address, you can access another Internet computer, such as a Web server.
- Other people on the Internet can obtain information about or access to your computer via a public IP address. ▪

Public IP addresses are visible to the public.

The option stating that public IP addresses are publicly registered with the Internet Service Provider (ISP) is incorrect. Public IP addresses are registered with the Internet Assigned Numbers Authority (IANA). Since 1998, InterNIC has been primarily responsible for allocating domain names and IP addresses under the governance of the Internet Corporation for Assigned Names and Numbers (ICANN) body, a U.S. non-profit corporation that was created to oversee work performed by the Internet Assigned Numbers Authority (IANA).

The option stating that 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255 are the range of public IP addressing is incorrect. These ranges belong to private IP addressing.

The option stating that private addresses are allocated by the IANA is incorrect. Private IP address are not managed, but are used by private organizations as they see fit. The IANA is governed by ICANN, and its primarily role is to allocate overseas global IP addresses from the pools of unallocated addresses, as well as DNS root zone management.

Objective:

Network Fundamentals Sub-

Objective:

Describe the need for private IPv4 addressing

References:

[Cisco > Support > IP Addressing http://www.debianadmin.com/private-and-public-ip-addresses-explained.html](http://www.debianadmin.com/private-and-public-ip-addresses-explained.html)

QUESTION 216

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:
[Cisco > Home > Support > Technology Support > IP > IP Routing > Configure > Configurations Examples and Technotes > How OSPF Injects a Default Route into a Normal Area](#)

QUESTION 217

Which Cisco IOS command is used to provide a description to an interface?

- A. description
- B. interface-description
- C. interface description
- D. description interface number

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The description command is used to provide a description to an interface. It is not a mandatory configuration. However, if you have configured the description for an interface, anyone who is working on the router can easily identify the purpose of the interface. Following is an example of the description command:

```
RouterA(config)# interface s0
```

```
RouterA(config-if)# description AT&T T1 to Internet
```

All the other options are syntactically incorrect.

Objective:
Infrastructure Management Sub-
Objective:
Perform device maintenance

References:
[Cisco > Cisco IOS Voice Command Reference > description](#)
[Tech Republic > Articles > Cisco administration 101: Five interface commands you should know](#)

QUESTION 218

What is the broadcast address for subnet 172.25.4.0/23?

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

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

Explanation:

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

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

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

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

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

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

References:

[Cisco > Design Tech Notes > IP Routing > IP Addressing and Subnetting for New Users > Understanding IP Addresses > Document ID: 13788](#)

QUESTION 219

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 220

Which is the valid broadcast ID for the IP address 192.24.134.12 with a subnet mask of 255.255.255.128?

- A. 192.24.134.127
- B. 192.24.134.128
- C. 192.24.134.129
- D. 192.24.134.131

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

192.24.134.127 is the valid broadcast ID for the IP address 192.24.134.12 with a subnet mask of 255.255.255.128. The valid range for the IP address 192.24.134.12 with a subnet mask of 255.255.255.128 is 192.24.134.1 - 192.24.134.126. The subnet ID is 192.24.134.0.

Subnetting allows you to split single and large subnets defined by Class A, B, and C IP addresses into multiple subnets with smaller IP address host ranges. Subnetting allows efficient use of IP addressing space, which has become a scarce resource.

To subnet an existing network, you will use host bits to split the IP address into multiple logical subnets. For example, if you use three bits of the host ID for subnetting, you have created $2^3 = 2 \times 2 \times 2 = 8$ subnets. Remaining bits of the host ID in decimal form will form the number of hosts on each subnet.

All other options are incorrect as these IP addresses fall in other subnets.

192.24.134.128 is the network ID for the next subnet created when using a mask of 255.255.255.128 on the class C network 192.24.134.0. The following network IDs are created when you use a mask of 255.255.255.128 on the class C network 192.24.134.0: ▪ 192.24.134.0 - Valid range 192.24.134.1-192.24.134.126, 192.24.134.127 is the broadcast

▪ 192.24.134.128 - valid range 192.24.134.129-192.24.134.254, 192.24.134.255 is the broadcast

192.24.134.129 and 192.24.134.131 are both valid addresses in the second subnet created, that is, the 192.24.128.0 network.

Objective:

Network Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

[Cisco > Technology Support > IP > IP Routing > Design Technotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses](#)

QUESTION 221

Which of the following commands will let you see the current operating mode for a switch port?

- A. show interface fastethernet0/1 detail
- B. show controllers fastethernet0/1
- C. show interface fastethernet0/1 status
- D. show interfaces fastethernet0/1 switchport

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show interfaces switchport command is used to verify the operational and configured status of a switch port. The output of the command is follows:

```
switch# show interfaces fastethernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<<output omitted>>
```



This output indicates that the operational mode of the port is "static access," which means the port is currently operating as an access port.

The show controllers command is used to view hardware-related information on router and switch interfaces. It is useful for troubleshooting and diagnosing issues with interfaces. It does not display the operational status of the switch port.

The show interface fastethernet0/1 detail and show interface fastethernet0/1 status commands are incorrect because they are not valid Cisco IOS commands.

Objective:

Infrastructure Management Sub-

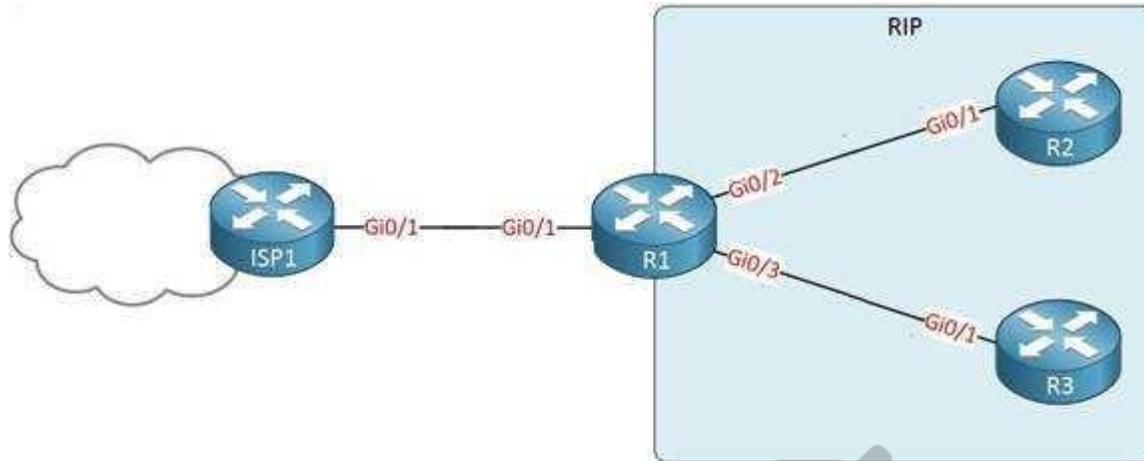
Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

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

QUESTION 222

Your network is configured as shown in the following exhibit. When you trace traffic sourced from R3 destined for a LAN network off of R2 (not shown in the diagram), you see the traffic is being forwarded from R1 to ISP1 rather than to R2.



Which of the following issues could NOT be causing this behavior?

- A. The network command has not been executed on the interface leading to the LAN off R2
- B. The passive interface command has been issued on the Gi0/4 interface of R1
- C. A default route exists on R1 that leads to ISP1
- D. RIPv2 has not been enabled on R2

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This issue would NOT be caused by executing the passive interface command on the Gi0/4 interface of R1. This command prevents the advertisement of RIP routes on that interface. If that command had been issued, the traffic would not be forwarded to R1 because R3 would not know about the route to the LAN off of R2. This command would also prevent R3 from knowing about the default route to ISP1. Since the traffic is being routed to ISP1, this command must not have been executed.

All of the other options could potentially because traffic destined for R2 to be forwarded from R1 to ISP1, rather than to R2.

It is true that a default route exists on R1 that leads to ISP1. If this default route did not exist, the traffic destined for R2 would simply be dropped at R1 instead of being forwarded to ISP1.

If the network command has not been executed on the interface leading to the LAN off of R2, the network leading to the LAN off R2 would not be advertised by R2.

That would make R1 unaware of this destination. In that case, R1 would use the default route to send traffic destined for R2 to ISP1. We know such a default route must exist, or the traffic would simply be dropped at R1.

If RIPv2 has not been enabled on R2, R2 would not be receiving or advertising any RIP routes. When the packets destined for the network off of R2 arrive at R1, R1 will not have a route to that network. In that case R1 will forward the traffic to ISP1 using the default route.

Objective:

Routing Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)

References:

[Cisco > Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > How Does the Passive Interface Feature Work in EIGRP?](#)

[Networkers-Online > Routing > IGP > EIGRP > Passive-interface command behavior in RIP, EIGRP & OSPF](#)

QUESTION 223

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

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

- A. traceroute
- B. traceroute
- C. extended ping
- D. ping

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

```
Type escape sequence to abort.  
Tracing the route to 33.0.0.4  
  
 1 11.0.0.2 4 msec 4 msec 4 msec  
 2 24.0.0.3 20 msec 16 msec 16 msec  
 3 33.0.0.4 16 msec * 16 msec  
  
Jan 20 16:42:48.611: IP: s=12.0.0.1 (local), d=33.0.0.4 (Serial0), len  
28,  
sending  
Jan 20 16:42:48.615: UDP src=39911, dst=33434  
Jan 20 16:42:48.635: IP: s=11.0.0.2 (Serial0), d=11.0.0.1 (Serial0), len  
56,  
rcvd 3  
Jan 20 16:42:48.639: ICMP type=11, code=0
```

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

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

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

Objective:

Routing Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

[Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > traceroute](#)

[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 224

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:

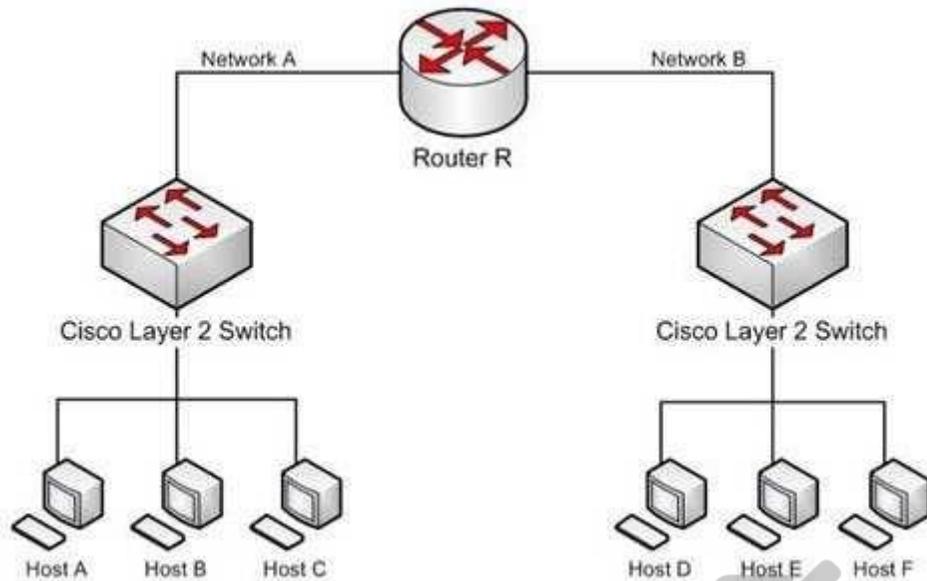
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

[Cisco > Support > Cisco IOS Software > Configuring EIGRP](#)

QUESTION 225

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 required. 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.msp>

<http://kb.iu.edu/data/ajfx.html>

QUESTION 226

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. 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 227

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 228



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
Serial10/0      16.2.0.1    Yes   manual up
Serial10/1      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 learned 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 229

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 230

Which command would be used to list the timers, version of spanning tree and the bridge ID of the local and designated switch for a specific VLAN on a Cisco Catalyst 2950 series switch?

- A. show spanning-tree vlan vlan-id
- B. show vlan database
- C. show vlan vlan-id
- D. show vlan brief



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show spanning-tree vlan vlan-id command is correct because this command shows timers, version of spanning tree, and the bridge ID of the local and designated switches for a specific VLAN on a Cisco Catalyst 2950 series switch.

The show vlan id vlan-id command is incorrect because it will show only the ports assigned to each VLAN.

The show vlan database command is incorrect because this is not a valid Cisco IOS command.

The show vlan brief command is incorrect because this command is used view the entire VLAN database, and does not provide information for a specific VLAN.

Objective:

Infrastructure Management Sub-

Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

[Cisco > Cisco IOS LAN Switching Command Reference, Release 12.4 > show vlan](#)

QUESTION 231

Which two are TRUE of straight-through cable? (Choose two.)

- A. The wires on the cable are crossed over.
- B. It is also known as a patch cable.
- C. You can connect two routers using a straight-through cable.
- D. You can connect a hub to a switch using a straight through cable.
- E. You can connect a switch to a router using a straight through cable.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A straight-through cable is also known as a patch cable, and a straight-through cable is used to connect a switch to a router. The following are the characteristics of a straight-through cable:

- It is a twisted-pair copper wire cable.
- The RJ-45 connectors at both ends have the same conductor arrangement.
- It is also known as a patch cable.
- You can connect a switch to a router using a straight-through cable.
- You can connect a router to a hub or a workstation to a hub using a straight-through cable. All the other options are incorrect because they are the characteristics of a crossover cable.

Objective:

Network Fundamentals Sub-

Objective:

Select the appropriate cabling type based on implementation requirements

References:

[Cisco > Support > Product Support > Routers > Cisco 10000 Series Routers > Troubleshoot and Alerts > Troubleshooting Technotes > Ethernet 100BaseTX and 10BaseT Cables: Guidelines and Specifications](#)

QUESTION 232

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 233

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 234

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

Routing Protocol	Cost
RIP	5
OSPF	25
EIGRP	2269571

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

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

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

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

Objective:

Routing Fundamentals Sub-

Objective:

Describe how a routing table is populated by different routing information sources

References:

[Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > Route Selection in Cisco Routers](#)

QUESTION 235

SwitchB receives a frame with the following fields:

Source MAC	Destination MAC	Source IP	Destination IP
00c0.57ce.ce33	00c0.aab3.1693	192.168.5.5	192.168.5.9

Below is the partial output of the **show mac-address table** command as executed on SwitchB:

```
Destination Address Address Type VLAN Destination port
00c0.57ce.ce33 Dynamic 1 FastEthernet0/4
00c0.566e.5858 Dynamic 1 FastEthernet0/5
00c0.45ee.eed4 Dynamic 1 FastEthernet0/7
00c0.aab3.1693 Dynamic 1 FastEthernet0/10
```

How will SwitchB handle the frame it just received?

- A. It will forward the frame out all ports
- B. It will forward the frame out FastEthernet0/4 only
- C. It will drop the frame
- D. It will record the source MAC address
- E. It will forward the frame out FastEthernet0/10 only



Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

SwitchB will forward the frame out FastEthernet0/10 only. The MAC address table indicates that the switch has the destination MAC address in its table and the destination is located on switch port FastEthernet 0/10, therefore it will switch the frame to that interface.

It will not forward the frame out all ports. It will only do that when it receives a frame for which it knows no destination and then it will forward it out all ports except the one on which it arrived. For example if it were sending a frame to 00c0.5658.d26e, which is nowhere to be found in the table and the frame arrived on port FastEthernet0/10 it would send the frame to every port except FastEthernet0/10.

It will not forward the frame out FastEthernet0/4. The MAC address located on that port is 00c0.57ce.ce33, which means that is the port on which the frame arrived.

It will not drop the frame. It will not drop the frame when it has the destination in its MAC table.

It will record the source MAC address. That address is already present in the table.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Describe and verify switching concepts

References:

[Cisco Documentation > Internetworking Case Studies > LAN Switching](#)

QUESTION 236

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

For example: `ip nat pool test 172.28.15.1`

`172.28.15.1 prefix 24`

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

```
ip nat inside source list 3 interface serial 0 overload
```

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



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

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

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

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

Objective:

Infrastructure Services Sub-

Objective:

Configure, verify, and troubleshoot inside source NAT

References:

[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 237

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 238

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 239

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 240

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 241

A newly implemented IP-based video conferencing application is causing the network to slow down.

Which OSI layer needs to be addressed to resolve the problem?

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

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

Objective:

Network Fundamentals Sub-

Objective:

Apply troubleshooting methodologies to resolve problems

References:

[Cisco Documentation > Internetworking Technology Handbook > Internetworking Basics > Open System Interconnection Reference Model](#)

QUESTION 242

Which of the following commands could you use to verify the type of serial cable you are connected to (DCE or DTE)?

- A. show interfaces
- B. show controllers
- C. show ip interface
- D. show interface dce
- E. show interface switchport

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show controllers command provides hardware-related information used to troubleshoot and diagnose issues with Cisco router interfaces. The output of the command is as follows:

```
routerA# show controllers serial 0
```

```
HD unit 1, idb = 0x1C44E8, driver structure at 0x1CBAC8 buffer
size 1524 HD unit 1
V.35 DTE cable, clock rate 64000
```

The preceding output indicates that a V.35 DTE cable is currently connected to interface Serial 0, and that a clock rate of 64000 bps has been detected from the DCE (the other side of the serial link). When the other end is a CSU/DSU, as is usually the case, the clock rate is provided by the CSU/DSU. The clocks stopped portion of the following output would indicate that a clock rate has not been detected from the DCE:

```
routerA# show controllers serial 0
HD unit 1, idb = 0x1C44E8, driver structure at 0x1CBAC8 buffer
size 1524 HD unit 1
V.35 DTE cable, clocks stopped
```

This condition would be rectified by configuring a clock rate on the DCE router.

The show interfaces, show ip interface, and show interface switchport commands do not display any hardware-related information, such as connected cable types.

The show interface dce command is incorrect because this is not a valid Cisco IOS command.

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



References:

QUESTION 243

You are the network administrator for your company. You have been assigned the task of configuring an appropriate IP addressing scheme in the network.

Assuming that the network address is 192.16.100.0/28, what will be the number of hosts per network in this scenario?

- A. 2
- B. 6
- C. 14
- D. 30

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this scenario, there will be 14 hosts per network. The formula for calculating the number of hosts on a subnet is $2^n - 2$, where n is the number of host bits in the summary mask. The n can be calculated by subtracting host bits from the total number of bits in a subnet mask (32). In this case, n would be $32 - 28 = 4$. Therefore, the formula to calculate the number of bits in this scenario would be:

$$2^{(32 - 28)} - 2 = 2^4 - 2 = 14 \text{ hosts}$$

You always subtract 2 from 2^n because the all-zero-bit address is reserved for the network address (called the network ID) and the all-one-bit address is reserved for the broadcast address.

The 192.16.100.0/28 network address would not have 30 hosts per network. The 192.16.100.0/27 network address would actually yield 30 hosts per network. In this case, n would be $32 - 27 = 5$, so the number of host bits in the subnet mask would be $32 - 2$, which is equal to 30.

The 192.16.100.0/28 network address would not have 6 hosts per network. The 192.16.100.0/29 network address would yield 6 hosts per network. In this case, n would be $32 - 29 = 3$, so the number of host bits in the subnet mask would be $8 - 2$, which is equal to 6.

The 192.16.100.0/28 network address would not have 2 hosts per network. The 192.16.100.0/30 network address would yield 2 hosts per network. In this case, n would be $32 - 30 = 2$, so the number of host bits in the subnet mask would be $4 - 2$, which is equal to 2.

Objective:

Network Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

[Cisco > Technology Support > IP > IP Routing > Design Technotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses](#)

QUESTION 244

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 245

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 246

Which feature is NOT provided by flow control?

- A. buffering
- B. windowing
- C. full duplex transmission
- D. source-quench messaging

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The full duplex mode of transmission is not provided by flow control. Full duplex transmission is an Ethernet concept where hosts are able to send and receive at the same time. There are no collisions in a full-duplex Ethernet network. A dedicated switch port is required for each node in a full-duplex Ethernet network. Both the host's NIC and the switch port must be capable of operating in full-duplex mode. When full duplex is implemented, no collisions will occur on the link between the switch and the device. That will be one error condition that can be removed from consideration when troubleshooting a full duplex link.

Flow control is a function that prevents network congestion. It does so by ensuring that the transmitting device does not flood the receiving device with data. The following statements are true regarding flow control:

- Controls the amount of data which the sender can send to the receiver.
- Uses buffering, transmitting source-quench messages, and windowing to handle network congestion.
- Determines the rate at which the data is transmitted between the sender and receiver. ▪

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

Flow control generally operates at the Transport layer in the OSI model. The Transport layer is responsible for error-free and sequential delivery of data. This layer is used to manage data transmission between devices.

Buffering is a method by which network devices use to save temporary overflows of excess data into the memory. The data is stored in the memory until it is processed.

Source-quench messages are used by the devices that receive the data to avoid buffer overflow.

Windowing is a scheme in which an acknowledgement is required by the source device from the destination after the transmission of a fixed number of packets.

Objective:

Network Fundamentals Sub-

Objective:

Compare and contrast OSI and TCP/IP models

References:

[Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Internet Protocols > TCP](#)

QUESTION 247

Which device creates broadcast domains and enables communication across separate broadcast domains?

- A. router
- B. switch
- C. hub
- D. access points

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A router allows communication across separate broadcast domains. A broadcast domain is a group of hosts and network devices in which a broadcast frame sent by one host can be received by all of the other hosts in the broadcast domain. A router determines the path to other destination networks, and forwards data packets to the next hop along this path. A router operates at Layer 3 of the Open System Interconnect (OSI) layered communication model and uses an Internet Protocol (IP) address hierarchy to identify and route data through source and destination devices.

A switch does not allow communication across separate broadcast domains. A switch creates collision domains and enables communications across different collision domains. A collision domain is a logical group of hosts and network devices where packets can potentially collide with one another, causing a communications disruption. Switches forward broadcasts so they do not form a separate broadcast domain unless Virtual LANs (VLANs) are created.

A hub does not allow communication across separate broadcast domains. A hub transmits frames, which means that they neither form separate collision or broadcast domains nor allow communication across these domains. Hubs are multiport devices that allow consolidation of various LAN segments and amplify signals that pass through them. Hubs operate at OSI Layer 1.

An access point does not allow communication across separate broadcast domains. Access points (APs) are OSI Layer 2 wireless hubs that allow client hosts to connect to the backbone network wirelessly.

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 248

Which of the following protocols is responsible for negotiating upper-layer protocols that will be carried across a Point-to-Point Protocol (PPP) connection?

- A. LCP
- B. NCP
- C. LMI
- D. ISDN

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Network Control Protocol (NCP) is responsible for negotiating upper-layer protocols that will be carried across the PPP connection. NCP defines how the two PPP peers negotiate with the network layer protocols, such as IP and IPX, which will be used across the PPP connection.

Link Control protocol (LCP) is not responsible for negotiating upper-layer protocols that will be carried across a PPP connection. Link Control protocol (LCP) has the primary responsibility of negotiating and maintaining the PPP connection. LCP, defined in Request for Comments (RFCs) 1548 and 1570, has the primary responsibility to establish, configure, authenticate, and test a PPP connection. LCP negotiates the following when setting up a PPP connection:

- Authentication method used (PAP or CHAP), if any
- Compression algorithm used (Stacker or Predictor), if any
- Callback phone number to use, if defined
- Multilink; other physical connections to use, if configured

Local Management Interface (LMI) is not responsible for negotiating upper-layer protocols that will be carried across the PPP connection. LMI is a characteristic of a frame relay connection. There are three types of LMIs supported by Cisco routers:

- Cisco
- ANSI Annex D
- Q933-A Annex A



LMI has nothing to do with PPP connections.

Integrated Services Digital Network (ISDN) is a type of WAN connection and has nothing to do with PPP connections.

Objective: WAN

Technologies Sub-

Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

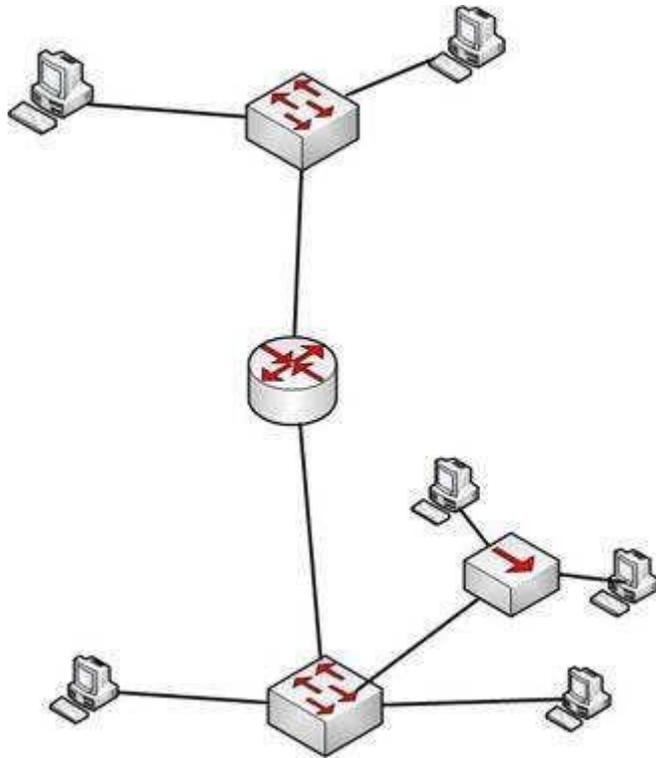
[Cisco > Internetworking Technology Handbook > Point-to-Point Protocol](#)

[Cisco > Support > Technology Support > WAN > Point-to-Point Protocol \(PPP\) > Design > Design Technotes > Understanding and Configuring PPP CHAP Authentication > Document ID: 25647](#)

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 12: Point-to-Point WANs, pp. 436-441.

QUESTION 249

How many collision and broadcast domains are in the network shown below?



- A. 4 collision domains and 3 broadcast domains
- B. 7 collision domains and 2 broadcast domains
- C. 8 collision domains and 1 broadcast domain
- D. 6 collision domains and 2 broadcast domains

Correct Answer: B

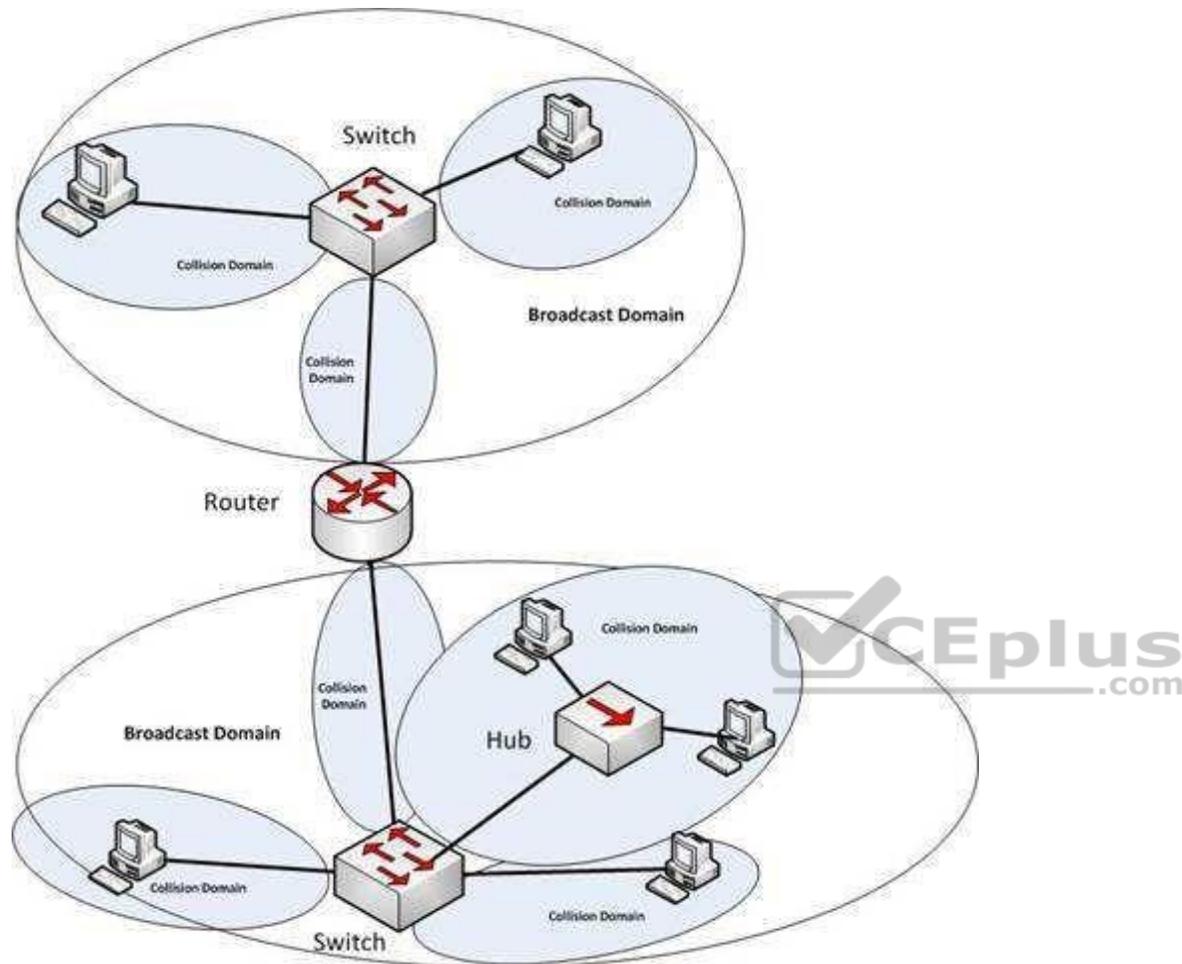
Section: (none)

Explanation

Explanation/Reference:

Explanation:

There are 7 collision domains and 2 broadcast domains. They are labeled as shown below. Each router interface makes a broadcast domain and each switch interface creates a collision domain. The hub interfaces do neither.



Objective:
 Routing Fundamentals Sub-
 Objective:
 Describe the routing concepts

References:
[Internetwork Design Guide -- Designing Switched LAN Internetworks > Comparison of LAN Switches and Routers](#)

QUESTION 250

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 a 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 251

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 252

Which command would you use to see which interfaces are currently operating as trunks?

- A. show interface switchports
- B. show trunk interface

- C. show interfaces trunk
- D. show switchport trunk

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The show interfaces trunk command displays a list of interfaces currently operating as trunks, and their configuration (such as supported VLANs or frame tagging method). Sample output would resemble the following:

```
Switch# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gi0/1 desirable 802.1q trunking 1
Gi0/2 desirable 802.1q trunking 1

Port Vlans allowed on trunk
Gi0/1 1-4094
Gi0/2 1-4094
<<output omitted>>
```



This output indicates that switch ports Gi0/1 and Gi0/2 are both currently operating as trunks (Status), and that 802.1q frame tagging is being used on the trunk links.

The remaining options are incorrect because they are not valid Cisco IOS commands.

Objective:

Infrastructure Management Sub-

Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

QUESTION 253

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 msec
Retransmission pacing timer 110 msec
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 254

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 be 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 255

Which two statements are TRUE of default routes? (Choose two.)

- A. Default routes are used for routing packets destined only for networks that are listed in the routing table.
- B. Default routes are used for routing packets destined for networks that are not listed in the routing table.
- C. Default routes should not be used in a stub network.
- D. Default routes are ideal for use in stub networks.
- E. Network security is increased by using default routes.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Default routes are to route packets that are destined for networks not listed in the routing table. Also, default routes are ideal for use in stub networks. Stub networks are those that have only one adjacent router interface and therefore only one interface to send any packet, regardless of destination. When used in this fashion the default route will be the only route in the routing table.

The following statements are also true of default routes:

- A default route is also known as the gateway of last resort.
- The default route in Internet Protocol Version 4 (IPv4) is represented as 0.0.0.0/0.

The option stating that default routes are used to route packets destined only for networks that are listed in the routing table is incorrect. Default routes are used for routing packets that are destined for networks not listed in the routing table.

The option stating that default routes should not be used in a stub network is incorrect. Default routes are helpful in topologies where it is not necessary to learn specific networks, making them ideal for use in a stub network.

The option stating that network security is increased by using default routes is incorrect. Default routes are not concerned with enhancing network security.

Objective:

Routing Fundamentals Sub-

Objective:

Describe the routing concepts

References:

[Cisco > Technology Support > IP > IP Routing > Design > Design Technotes > Configuring a Gateway of Last Resort Using IP Commands > Document ID: 16448 > Flag a Default Network](#)



QUESTION 256

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 Infrfce	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 Infrfce: 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 257

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 258

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 259

Which Network Address Translation (NAT) term is used for the IP address that is assigned to a host on the inside network?

- A. Inside local address
- B. Inside global address
- C. Outside local address
- D. Outside global address



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An inside local address is the NAT term that is used to describe the IP address assigned to a host on the inside network. It is usually a private IP address.

An inside global address is the registered IP address assigned by the ISP, which represents one or more inside local IP addresses externally.

An outside local address is the IP address of an external host as it appears to the internal network.

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.

NAT enables companies to use one IP addressing scheme within their network but translate those IP addresses for external communication. Static NAT assigns a permanent one-to-one mapping of local addresses to global addresses. Dynamic NAT assigns address mappings by using a pool of available addresses. NAT overloading or Port Address Translation (PAT) reduces the number of global addresses required by allowing multiple local hosts to share a global address.

Objective:

Infrastructure Services Sub-

Objective:

Configure, verify, and troubleshoot inside source NAT

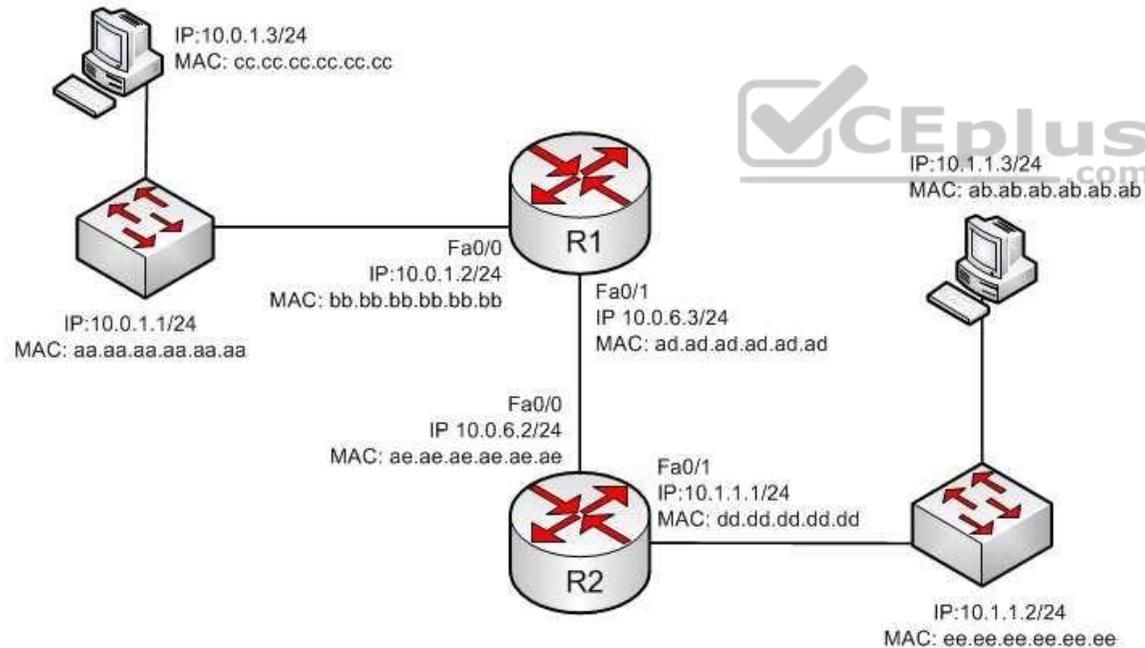
References:

[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 260

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. The router interface would then encapsulate the packet in a frame addressed to 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 Tcpiip. . . . . : 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 261

You have added a new router to your network using all of the default settings. You can connect to everything by IP address, but the router doesn't seem to be resolving names to IP addresses. The DNS server is in a directly connected network.

Which of the following is most likely the problem?

- A. You configured an incorrect IP address for the DNS server
- B. You configured an incorrect default gateway on the router
- C. You failed to execute the ip domain lookup command
- D. You failed to create an IP helper address

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The most likely problem is that you configured an incorrect IP address for the DNS server. Although it is impossible to know without executing the show run command, the other options can all be eliminated, making this the most likely option.

Even if the router has an incorrect default gateway, or has no default gateway configured, the router should be able to connect to resources by name if it can connect to them by IP address. The gateway will only be required if the DNS server is in a network not found in the routing table of the local router. Since the network containing the DNS server is directly connected, that network is automatically in the routing table.

The ip domain lookup command is enabled by default, so it does not need to be executed. If the scenario had not stated that all defaults were in place, it could be verified with the show run command as shown below, where line 4 indicates the ip domain lookup command is disabled:

```
routera# show run
<output omitted>
hostname routera

no ip domain lookup ip
domain name acme.com ip
name-server 192.31.1.6
```

It is not required to have an IP helper address for DNS to function for the router. It is only required by the non-routing devices connected to the router, and only for those that are not on the same network with their DHCP server.

Objective:

Infrastructure Services Sub-

Objective:

Troubleshoot client- and router-based DHCP connectivity issues

References:

QUESTION 262

You are the network administrator for your company. You wanted to connect the host computers to the switches.

Which cable should you use to ensure the connectivity?

- A. Straight-through cable
- B. Rollover cable
- C. Crossover cable
- D. Serial cable

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A straight-through cable is a normal four-pair cable with the same order of pin configuration on both ends. These are usually used to connect a computer to the switch or hub's Ethernet ports. The following table shows the pin layout of a straight-through cable:

Pin No.	Pin No.
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

A rollover cable, also known as rolled cable or Cisco console cable, is used to connect a computer terminal to the console port of a router. The cable pin order at one end of the cable is the reverse of the order at another end. Pin 1 is connected to pin 8, pin 2 to pin 7, and so on.

A crossover cable is used to connect two similar devices such as a computer to computer or a switch to a switch, and a computer to a router's Ethernet port.

A serial cable is used on a router's wide area network (WAN) interface to connect to the serial ports. Cisco serial cables generally have a male DB-25 connector on one end and a female DB-25 connector on the other.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

[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 263

Which protocol is responsible for negotiating and maintaining Point-to-Point Protocol (PPP) connections?

- A. LCP
- B. NCP
- C. BRI
- D. ISDN



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Link Control protocol (LCP) has the primary responsibility of negotiating and maintaining a PPP connection. LCP, defined in Request for Comments (RFCs) 1548 and 1570, has the primary responsibility to establish, configure, authenticate, and test a PPP connection. LCP negotiates the following when setting up a PPP connection:

- Authentication method used (PAP or CHAP), if any
- Compression algorithm used (Stacker or Predictor), if any
- Callback phone number to use, if defined
- Multilink; other physical connections to use, if configured

The ability to utilize compression, authentication, and multilink are three options that make PPP a popular choice for Layer 2 encapsulation over a WAN link.

Network Control Protocol (NCP) defines how the two PPP peers negotiate with network layer protocols, such as IP and IPX, will be used across the PPP connection. LCP is responsible for negotiating and maintaining a PPP connection whereas NCP is responsible for negotiating upper-layer protocols that will be carried across the PPP connection.

In summary, the three steps in the establishment of a PPP session are: ▪

Link establishment phase

- Optional authentication phase
- Network layer protocol phase

Basic Rate Interface (BRI) and Integrated Services Digital Network (ISDN) are not components of PPP, so these options are incorrect. BRI is a type of ISDN connection that contains three circuits, two 64K B or bearer channels, and one D or Delta channel. ISDN circuits are a type of WAN connection.

Objective: WAN

Technologies Sub-

Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

[Cisco > Internetworking Technology Handbook > Point-to-Point Protocol](#)

[Cisco > Support > Technology Support > WAN > Point-to-Point Protocol \(PPP\) > Design > Design TechNotes > Understanding and Configuring PPP CHAP Authentication > Document ID: 25647](#)

QUESTION 264

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 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 265

You need to set the Telnet password to "john" on a Cisco router. Which set of commands would you use?

- A. `Router(config)#line vty 0 4`
`Router(config-line)#login`
`Router(config-line)#password john`
- B. `Router(config)#line con 0`
`Router(config-line)#login`
`Router(config-line)#password john`
- C. `Router(config)#line vty 0 4`
`Router(config-line)#login`
`Router(config-line)#enable secret john`
- D. `Router(config)#line con 0`
`Router(config-line)#login`
`Router(config-line)#enable password john`



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The set of commands which would be used to configure the Telnet password to "john" on a Cisco router is:

`Router(config)#line vty 0 4`

`Router(config-line)#login`

`Router(config-line)#password john`

The line vty command is used to configure the router to enable Telnet access. By using this command, the router can be configured to accept one or more Telnet sessions.

The login and password parameters are the line configuration commands used to configure the password. The password command specifies the password and the login command instructs the router to require the password. By default, the login parameter is present in the configuration of the VTY lines. Because its presence indicates that a password is required for connecting to the VTY lines, if a password has not been configured on the VTY lines, a connection cannot be made. If an attempt were made to connect to the VTY line with the login parameter in effect and no password present, the following error message would be generated:

```
Router2# telnet 10.3.1.1
Trying 10.3.1.1Open

Password Required, but none set
[Connection to 10.3.1.1 closed by foreign host]
Router2#
```

The following set of commands would be used to configure the console password on a Cisco router, and so it is incorrect for this scenario.

```
Router(config)# line con 0
Router(config-line)# login
Router(config-line)# password john
```

The commands enable secret john and enable password john would be used to configure the enable secret password and the enable password for the router. However, they cannot be used to configure the Telnet password. Therefore, these options are incorrect.

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

References:

QUESTION 266

Which Cisco IOS command would produce the following output?

```
Serial0/0/0 is administratively down, line protocol is down
Hardware is GT96K Serial
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 HDLC, loopback not set,
Keepalive set (10 sec)
Last input never, output 0:00:14, output hang never
Last clearing of "show interface" counters 0:00:00
Input queue 0/40/0/0, (size/max/drops/flushes);Total output drops :81071
Queueing strategy:FIFO
Output Queue: 0/40 (size/max)
Five minute input rate 0 bits/sec, 0 packets/sec
Five 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 abort
145 packets output, 5084 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets, 0 restarts
<<output omitted>>
```

- A. show ip interface
- B. show ip interface brief
- C. show interfaces
- D. show interface brief

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

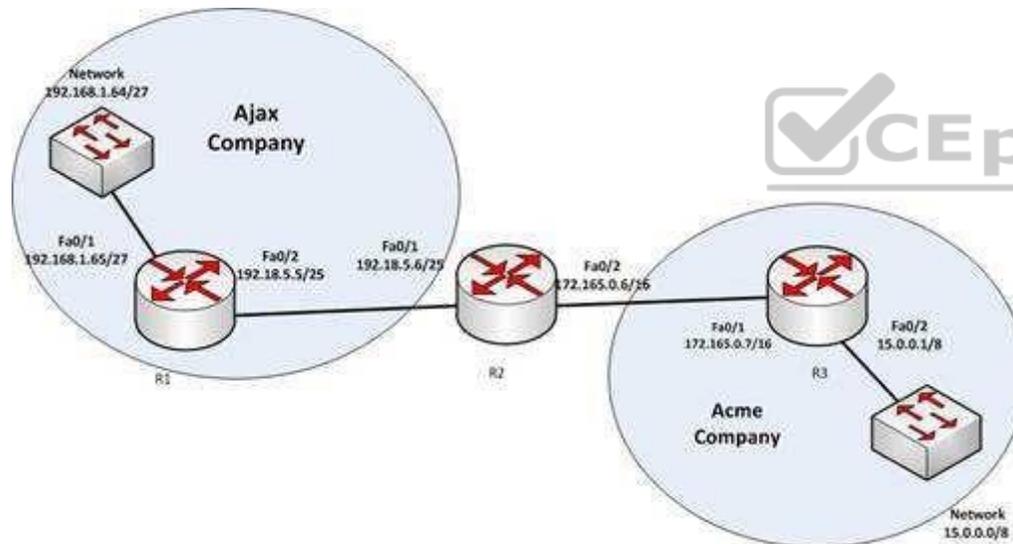
Explanation:

The output given in the question is produced with the show interfaces command. This command is used to view the statistics for the configured interfaces on the router. From the sample output, we can determine the following facts:

- The interface has not been enabled, as indicated by the first line Serial0/0/0 is administratively down. It is not ready to forward packets. To enable it, the no shutdown command should be entered.
- Line 3 shows that the subnet mask is 255.255.255.0.
- Line 3 shows that the IP address is 134.108.28.8, a public IP address.
- Line 6 shows that the encapsulation is HDLC, which is the default.
- The interface is NOT connected to a LAN, because it is a serial interface.

Two fields worth mentioning in the output of the show interfaces command are the no buffer and the ignored fields. The ignored field shows the number of received packets ignored by the interface because the interface hardware ran low on internal buffers. The no buffer field shows the number of received packets discarded because there was no buffer space in the main system. When either of these two counters begins to increment, it could be the result of a broadcast storm.

Since the show interfaces command displays the up/down state of the interfaces, it is a good command for troubleshooting. For example, any time users cannot access a resource that requires them to traverse a router, it is always a good idea to use show interfaces to take a quick look at the state of the interfaces. In the example diagram below, users cannot access the resource in the network of the Acme Company from the LAN in the Ajax Company. The first step would be to execute the show interfaces command in R1 to verify functionality of the interfaces on R1.



The show ip interface command is incorrect because this command is used to view whether the interfaces configured for Internet Protocol (IP) are usable. Following is a sample output of the show ip interface command:

```
GigabitEthernet0/3 is up, line protocol is up
Internet address is 10.2.1.1/16
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 unreachable 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
```



The show ip interface brief command is incorrect because this command provides an overview of all the interfaces configured for IP on the router. The following is sample output from the show ip interface brief command. It can be quite useful for troubleshooting as well. For example, if you cannot ping the Ethernet1 interface from a host on the Ethernet 0 LAN, you could determine from the output below that the Ethernet 1 interface is administratively down.

```
Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol
Ethernet0 12.17.10.5 YES NVRAM up up
Ethernet1 unassigned YES unset administratively down down
Loopback0 12.17.20.5 YES NVRAM up up
Serial0 12.17.30.5 YES NVRAM up up
```

The solution here would be to enter configuration mode for the interface Ethernet 1 and enable it with the no shutdown command.

The show interface brief command is incorrect because this command is not a valid Cisco IOS command.

Objective:

LAN Switching Fundamentals Sub-

Objective:

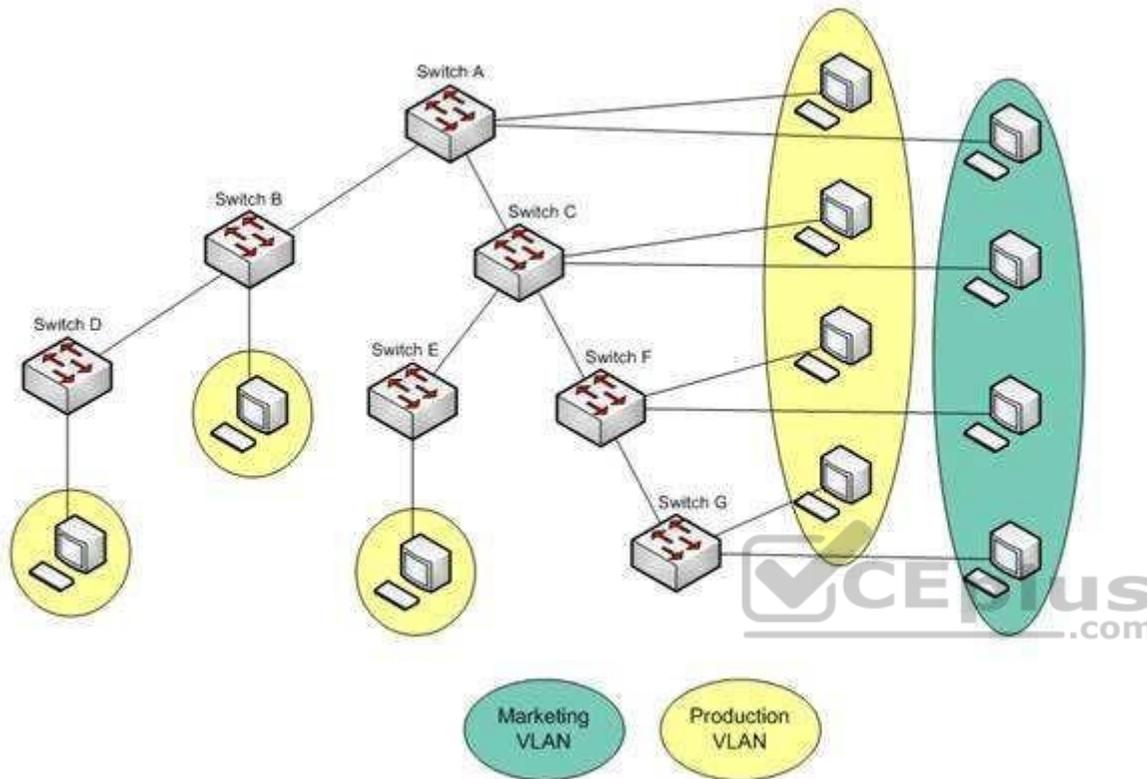
Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:



QUESTION 267

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

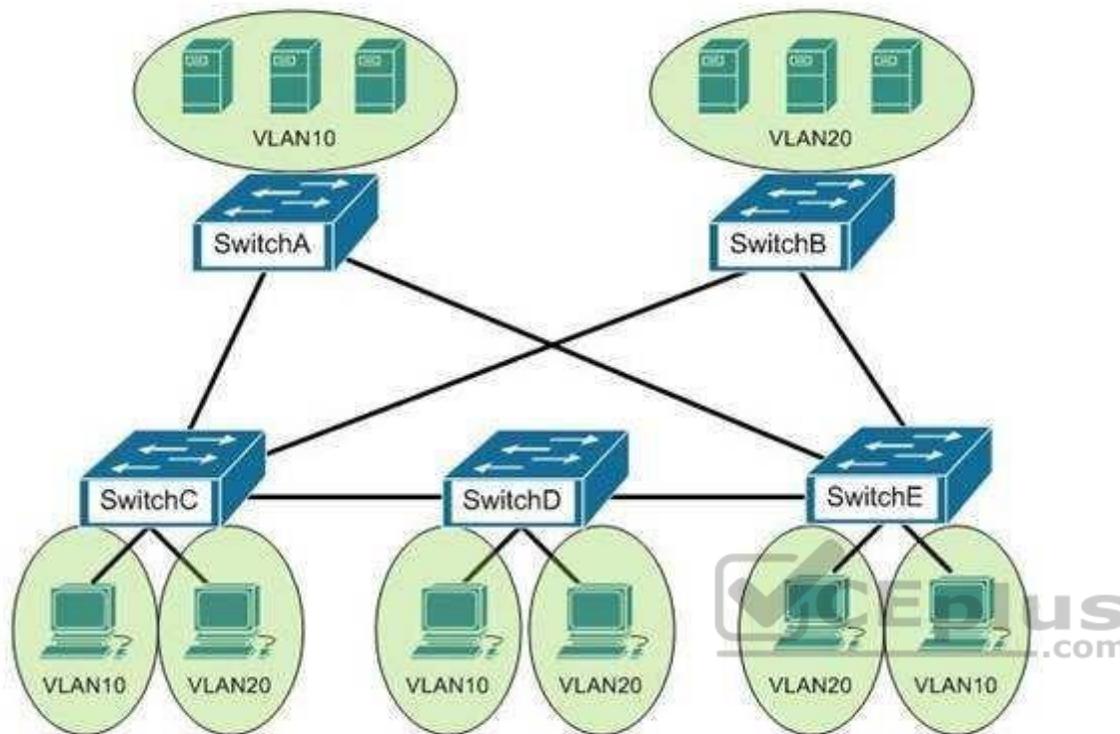
References:

[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 268

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 269

Which command is used on the Cisco Catalyst 2950 series switch to configure a port as a VLAN trunk port?

- A. switchport mode trunk
- B. set trunk on
- C. switchport trunk on
- D. trunk mode on

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The switchport mode trunk command is used on the Cisco Catalyst 2950 switch to configure a port as a VLAN trunk port. The syntax of the command is as follows:

Switch(config-if)# switchport mode trunk

Trunk links are required between devices in any situation where traffic from multiple VLANs will traverse the link. This is also true when using VTP on the switches and in that case, even if inter-VLAN routing is not required. For example, if two switches in a VTP domain are connected together via an access link with no router present, then when you create a new VLAN on one of the switches, it will NOT be learned by the other switch.

When you configure a trunk link, there are two choices for encapsulation: 802.1q, which is the industry standard, and ISL, which is Cisco proprietary and will only work when both ends are Cisco equipment. Both protocols perform a crucial role in inter-VLAN routing by tagging packets with the VLAN to which the packets belong.

The following commands should be issued to configure FastEthernet 0/1 to function as a VLAN trunk port and use 802.1q encapsulation:

```
Switch# configure
terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
```

When configuring a trunk link between a switch and switch, the above commands would be used in both switches. However, when a trunk link is configured between a router and a switch, the process is different on the router. On the router end, you must do the following:

1. Enable the physical interface hosting the trunk link.
2. Ensure that no IP address exists on the physical interface.
3. Create a subinterface for each VLAN on the physical interface.
4. Set the trunking protocol on each subinterface.
5. Configure an IP address on each subinterface.



The command set that would create a subinterface for VLAN 10, set the trunking protocol for the subinterface, and assign the subinterface an IP address is:

```
Router(config)#interface fastethernet 0/0
Router(config)#no ip address
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastethernet 0/0.1
Router(config-if)#encapsulation dot1q 10
Router(config-if)#ip address 192.168.5.1 255.255.255.0
```

The set trunk on, switchport trunk on , and trunk mode on commands are incorrect because these are not valid Cisco IOS commands.

Objective:

LAN Switching Fundamentals Sub-

Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

[Cisco Catalyst 2950 Desktop Switch Software Configuration Guide, 12.0\(5.2\)WC\(1\) > Creating and Maintaining VLANs > CLI: Configuring a Trunk Port](#)

[Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport mode](#)

QUESTION 270

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 www.vceplus.com - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com
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 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 271

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
VTP Version : 2
Configuration Revision : 62
Max VLAN support 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
```

```
Switch61# show vtp status
VTP Version : 2
Configuration Revision : 62
Max VLAN support locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Transparent
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
```

```
Switch62# show vtp status
VTP Version : 2
Configuration Revision : 62
Max VLANs support locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Client
VTP Domain Name : Corp
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
```

```
Switch63# show vtp status
VTP Version : 2
Configuration Revision : 63
Max VLAN support locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Client
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled
VTP V2 Mode : 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 Switch62 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:

QUESTION 272

Which Cisco IOS command would prompt for input in the following format?

```
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.142.23.10
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.
```

- A. ping 10.1.1.1
- B. ping
- C. traceroute
- D. tracert



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The extended ping command prompts the user for input in the format given in this scenario. The extended ping command is accessed by issuing a ping command without specifying an IP address. This causes the ping command to transit into extended ping command mode, where you can specify and modify various parameters, such as packet size, timeout, and repeat count.

The following code is a sample partial output of the extended ping command:

```
Router A#ping
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.142.23.10
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 true value of the extended ping command lies in the ability to ping FROM a different device than the one you are working from. As shown in the above output, you can specify the source address on line 8.

The ping 10.1.1.1 command is incorrect because it sends an ICMP "echo request" to the target host. In turn, the target host replies with the "echo reply" packets. When pinging from one device to another on the network, ICMP and Address Resolution Protocol (ARP) are used. ARP resolves an IP address to its associated MAC addresses.

The tracert command is incorrect because this command is used by Microsoft Windows, not Cisco. It is not a valid utility to run via the Cisco IOS command-line interface. The tracert command is similar to the traceroute Cisco utility as the tracert command tests the connectivity or "reachability" of a network device or host. It reports back a reply at each hop, allowing one to determine where the communication link is "broken".

The traceroute command is used to display the path that a packet follows to its destination. This command displays the IP address of each router in the path from the source to the destination address. Unlike the Microsoft tracert command, which uses the ICMP protocol, the Cisco traceroute command is based on User Datagram Protocol (UDP). The following code is the partial output of the traceroute command.

```
RouterA#traceroute 124.10.23.41

Type escape sequence to abort.
Tracing the route to 124.10.23.41

 0 121.10.1.3 6 msec 6 msec 6 msec
 1 134.10.10.13 30 msec 17 msec 14 msec
 2 32.1.2.4 36 msec * 23 msec
```

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

References:
[Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730](#)
[Cisco > Tech Notes > Understanding the Ping and Traceroute Commands > The Traceroute Command > Document ID: 12778](#)

QUESTION 273

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

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

Correct Answer: B
Section: (none)
Explanation



Explanation/Reference:

Explanation:

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

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

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

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

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

References:

[Cisco > Support > IPv6 Configuration Guide, Cisco IOS Release 15.2S > Chapter: IPv6 Unicast Routing](#)

[Cisco > Support > Cisco IOS IPv6 Command Reference > ipv6 unicast-routing](#)



<https://vceplus.com/>

