100-105.exam

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

Cisco

100-105

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

Version 1.0

Exam A

QUESTION 1
You 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:
Network Fundamentals

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

References:

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

QUESTION 2
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

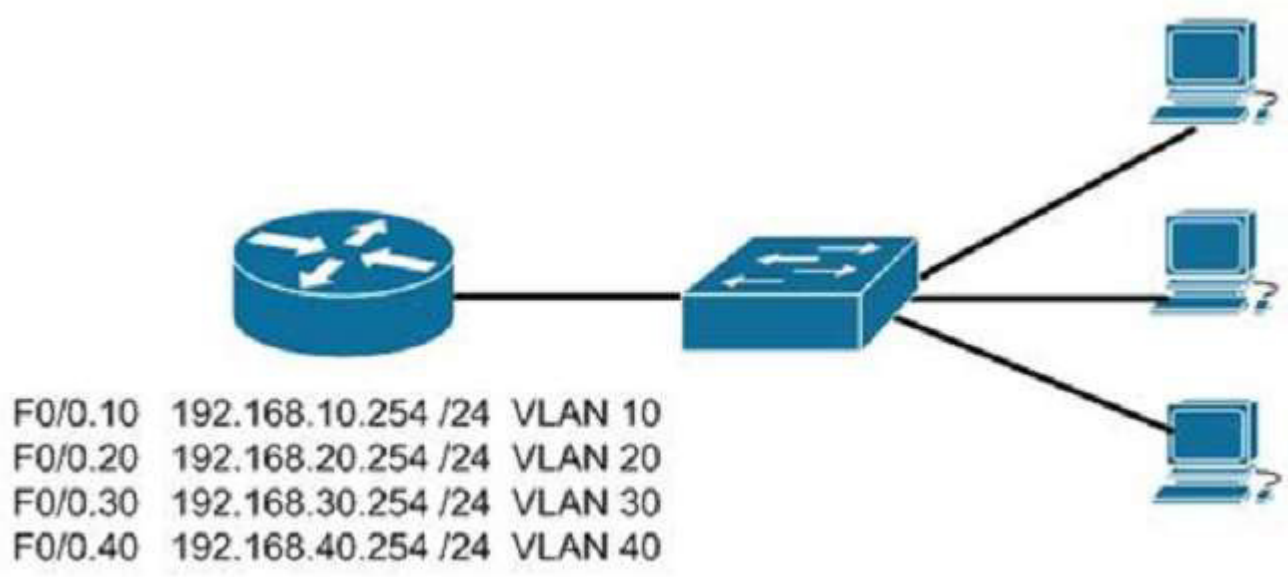
References:

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

QUESTION 3
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 range) spanning multiple switches

References:

https://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_s2.html#wp1105725

https://www.amazon.com/gp/product/1119092159/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&tag=transcender02-20&camp=1789&creative=9325&linkCode=as2&creativeASIN=1119092159&linkId=987d02c2e2801e3c4c082ea3b691f3ebChapter 15: ConfiguringInter-VLAN Routing

QUESTION 4
Which two statements are TRUE of routing? (Choose two.)

A. It is a Layer 2 function.
B. It is a Layer 3 function.
C. It is a forwarding technique used in packet-switched computer networks.
D. It works by broadcasting.
E. It refers to the determination of the path from the source to the destination in a network.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Routing is a Layer 3 function that refers to the determination of the path from the source to the destination in a network. The following statements are also true of routing:

- The basic routing function is the determination of the best routing path in an internetwork.
- Routing can use routing protocols to determine the best path to the destination with the help of routing metrics.
- A hop-by-hop routing model is used.

With the goals of routing in mind, each router will take two actions with regard to each packet it encounters:

- Identify the destination network address of each packet
- Inspect the routing table to select the best path to the destination network address

The option stating that routing is a Layer 2 function is incorrect because routing is a Layer 3 function. Bridging is a Layer 2 function.

The option stating that routing is a forwarding technique used in packet-switched computer networks is incorrect. Bridging is a forwarding technique used in packet-switched computer networks.

The option stating that routing works by broadcasting is incorrect. Routing is based on unicast methodology.

Objective:
Routing Fundamentals

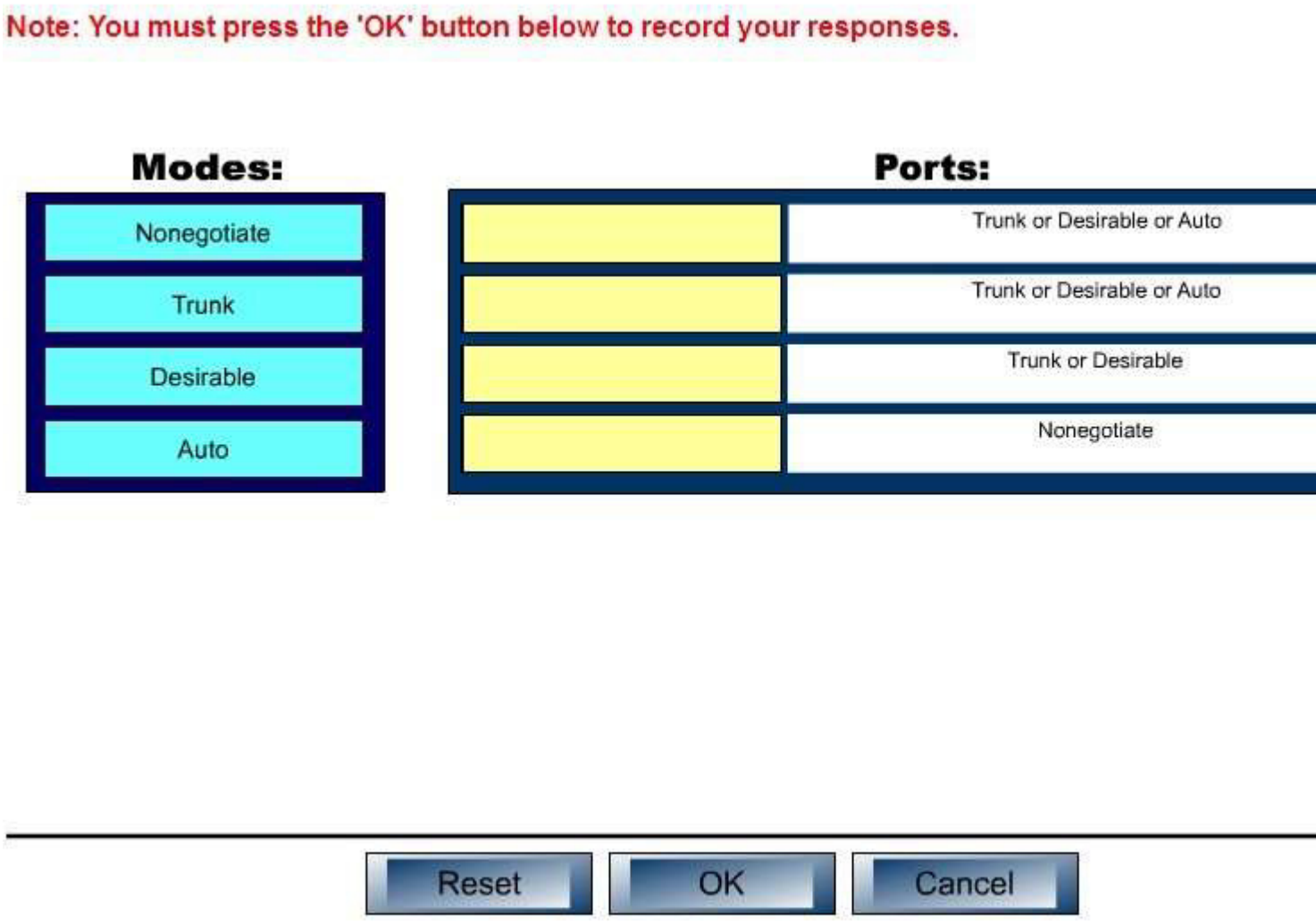
Sub-Objective:
Describe the routing concepts

References:

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

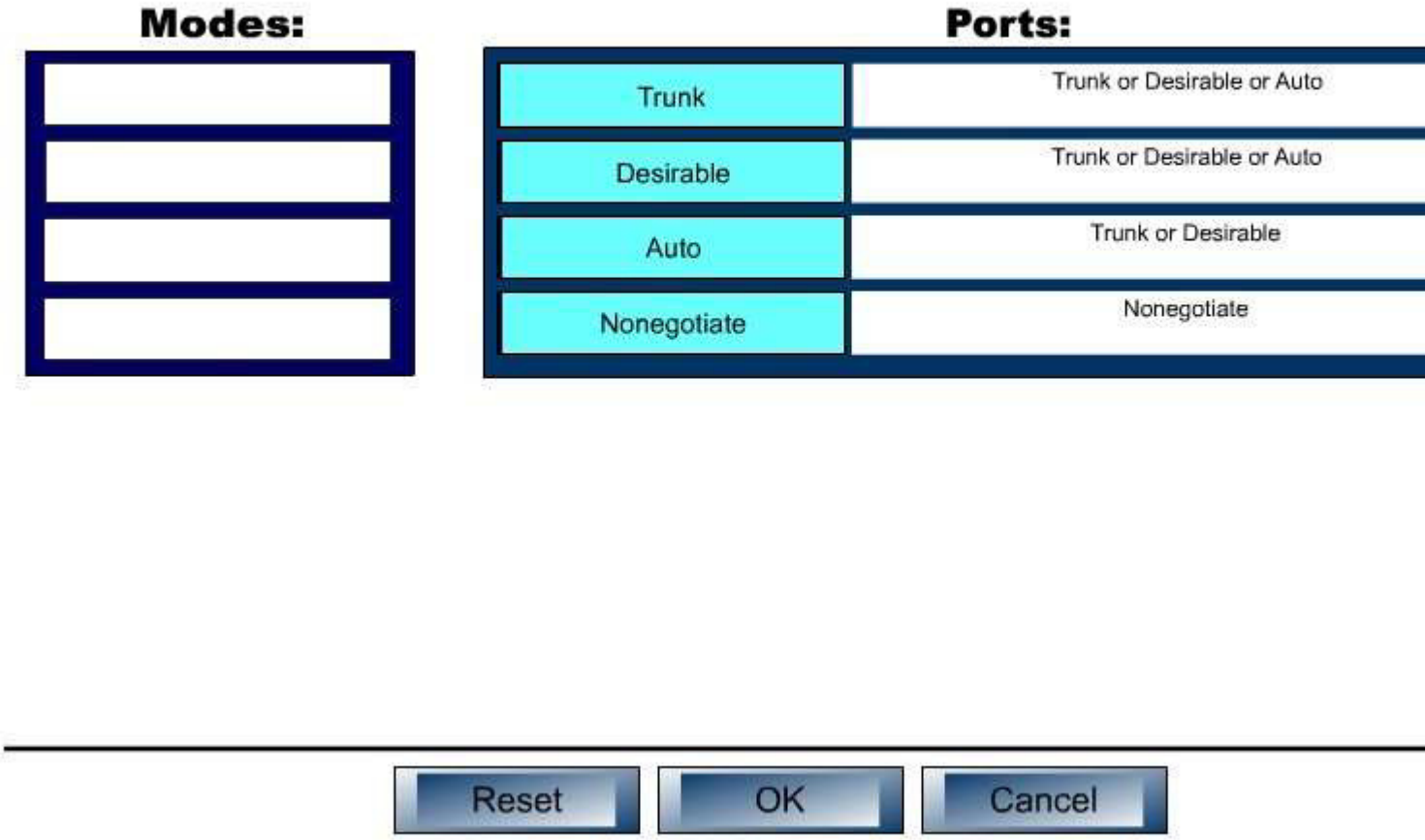
QUESTION 5
DRAG DROP
Match the Dynamic Trunking Protocol (DTP) configuration on the switch ports so that a trunk link can be established. (Click and drag the DTP modes on the left and place them with their corresponding port on the right.)

Select and Place:



Correct Answer:

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



Section: (none)
Explanation

Explanation/Reference:
Explanation:

There are five DTP modes:

- Trunk: Switch will establish trunk if other end port is configured as Trunk/Desirable/Auto.
- Dynamic Desirable: Switch will establish trunk if other end port is configured as Trunk/Desirable/Auto.
- Dynamic Auto: Switch will establish trunk if other end port is configured as Trunk/Desirable.
- Nonegotiate: Other end port should also be configured with Nonegotiate, or should be a device that does not support DTP.
- Access: No trunk establishment.

Objective:
LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer2 protocols

References:

QUESTION 6
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:

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

QUESTION 7
Which of the following commands is used to verify the link-local, global unicast, and multicast addresses of an IPv6 router?

A. show ipv6 neighbors (only link-local addresses)

B. show ipv6 route
C. show ipv6 protocols
D. show ipv6 interface

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show ipv6 interface command is used to verify the link-local, global unicast, and multicast addresses assigned to an IPv6-enabled router interface. The show ipv6 interface command displays information regarding that interface, such as the physical state, MTU, and IPv6 enable/disable state.

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

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

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

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

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

You can also notice in the sample output that the Fa0/1 interface belongs to three multicast groups: FF02::1, FF02::2, andFF02::1:FF5D:A031. The first two multicast groups refer to the all-host and all-router multicast groups, respectively. The third group, FF02::1:FF5D:A031, is the solicited-node multicast address. This address is created for every unicast or anycast address. A solicited-node multicast address is determined by assigning the least significant 24 bits of the unicast address to the least significant 24 bits of the FF02::1:FF00:0 address.

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

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

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

Objective:
Network Fundamentals

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

References:
https://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_14.html#wp2332322

https://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_15.html#wp2364932

https://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_15.html#wp2372269

https://www.cisco.com/c/en/us/products/ios-nx-os-software/enterprise-ipv6-solution/white-paper-listing.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-multicast.html

QUESTION 8
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 cdpcommand 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:

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

QUESTION 9
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 CDPv2advertisements 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

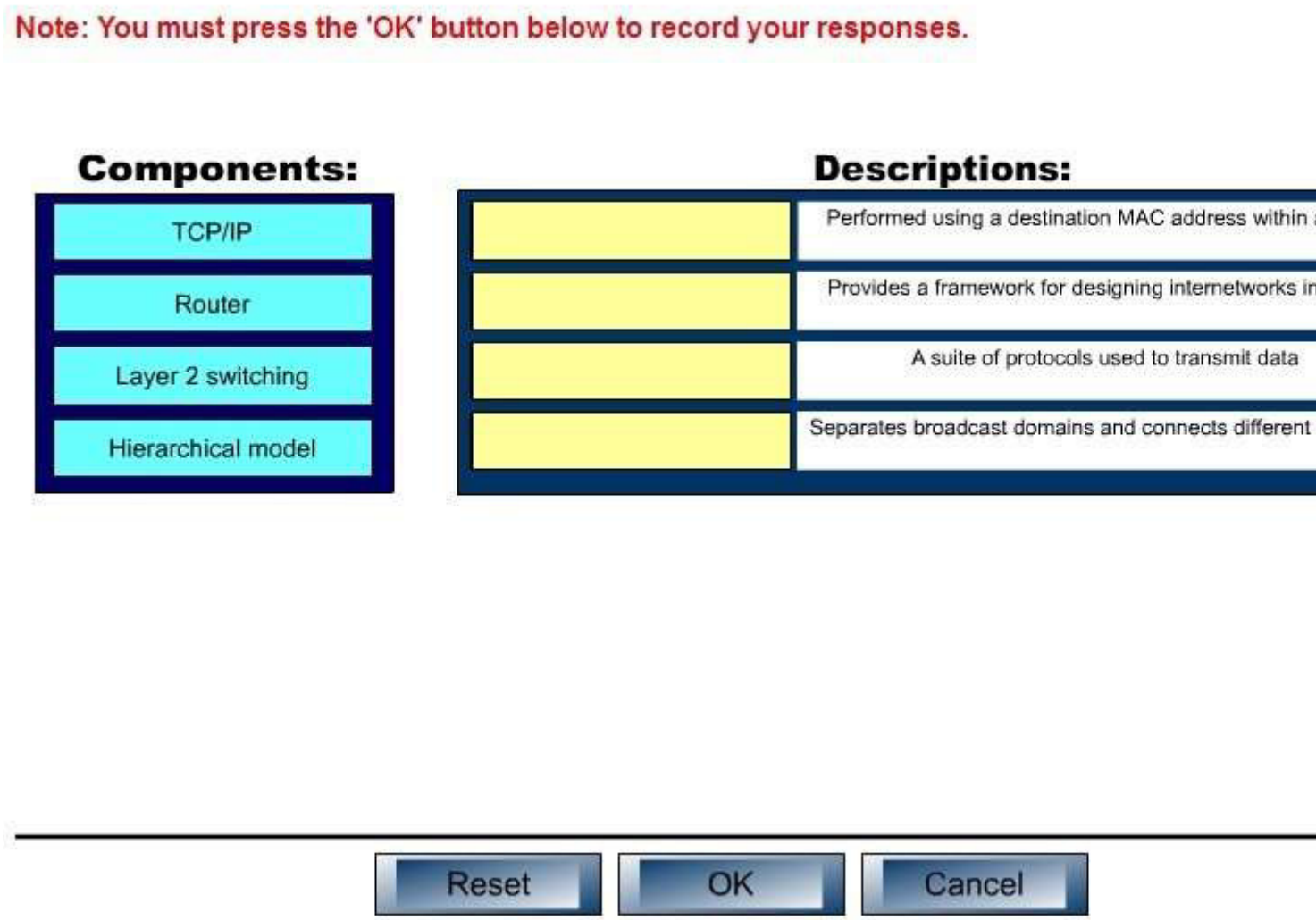
Sub-Objective:
Configure and verify Layer 2 protocols

References:

https://search.cisco.com/search?query=Cisco%20IOS%20Network%20Management%20Configuration%20Guide&locale=enUS&tab=Cisco

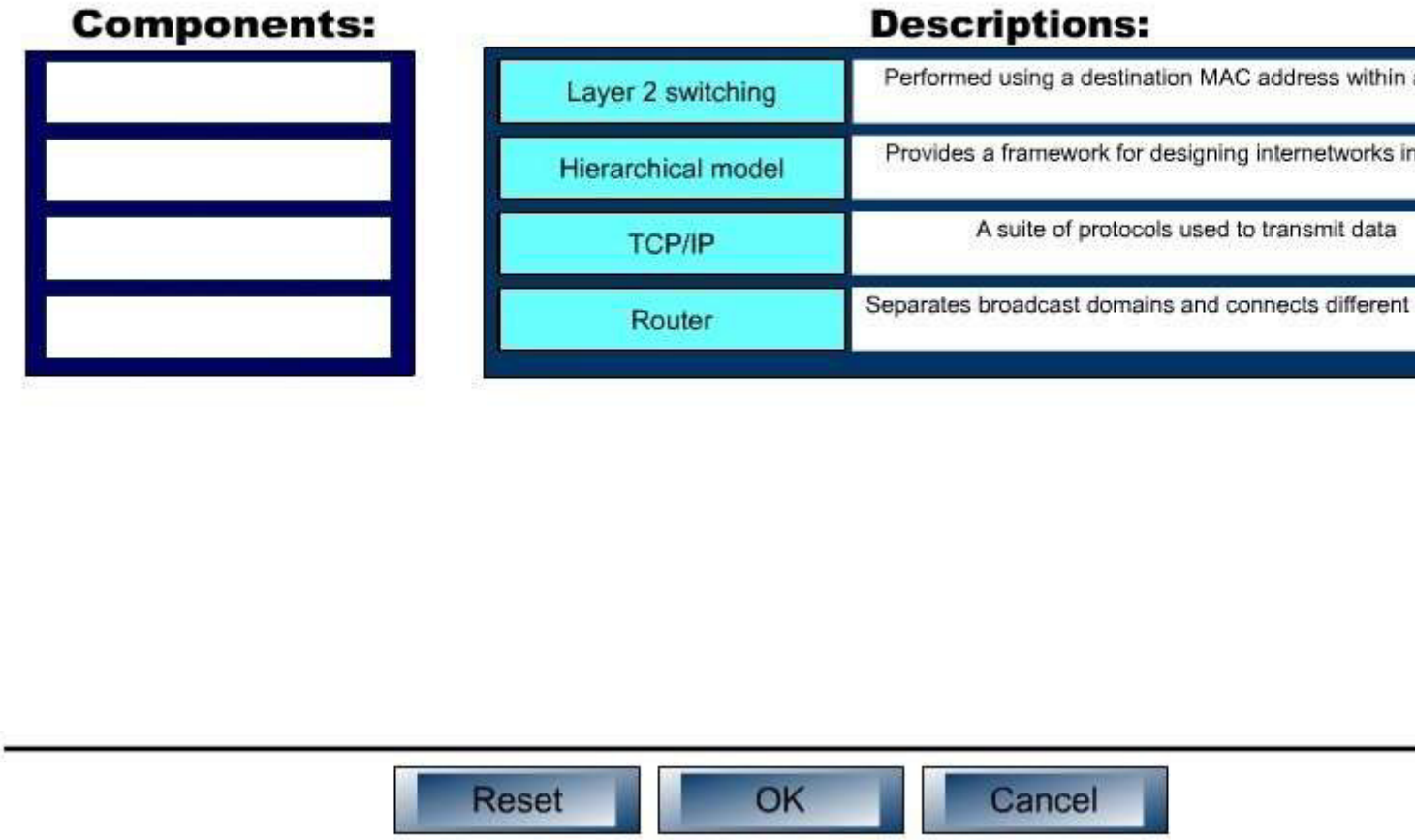
QUESTION 10
DRAG DROP
Click and drag the network components and functions to their corresponding descriptions on the right.

Select and Place:



Correct Answer:

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



Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following network components and functions should be matched to these corresponding descriptions:

- Transmission Control Protocol (TCP)/Internet Protocol (IP): TCP/IP is a suite of data communication protocols.
- Router: Separates broadcast domains while connecting different networks. Routers also provide a medium for connecting Local Area Network (LAN) and Wide Area Network segments.
- Layer 2 switching: Performed using a destination MAC address within a frame. In Layer 2 switching, switching is based on Media Access Control (MAC) addresses.
- Hierarchical model: Enables the designing of inter networks into layers. There are three layers in the hierarchical network design:
- Core layer: Provides high-speed data transfer between sites.
- Distribution layer: Includes LAN-based routers and Layer 3 switches and enables routing between Virtual Local Area Networks (VLANs).
- Access layer: Provides workgroup and end-user access, and is also referred to as the desktop layer.

Objective:
Network Fundamentals

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

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

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

QUESTION 11
Which access list statement will permit all HTTP sessions to subnet 192.168.144.0/24 containing Web servers?

A. access-list 110 permit udp any 192.168.144.0 eq 80
B. access-list10 permit tcp 192.168.144.0 255.255.255.0 eq www
C. access-list 110 permit tcp any 192.168.144.0 0.0.0.255 eq 80
D. access-list 10 permit udp any 192.168.144.0 255.255.255.0 eq 80
E. access-list 110 permit tcp 192.168.144.0 0.0.0.255 any eq 80
F. access-list 110 permit tcp any 192.168.144.0 0.0.0.0 any eq 80
G. access-list 110 permit tcp any 192.168.144.0 0.0.0.255 any eq 23
H. access-list 110 permit tcp 192.168.144.0 0.0.0.255 192.168.144.0 0.0.0.255 any eq 80

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The access-list 110permit tcp any 192.168.144.0 0.0.0.255 eq 80 command is syntactically correct. To permit HTTP sessions for a destination subnet 192.168.144.0/24, you will require an extended IP access list. Access list number 110 is in the range of extended IP access lists.

All source addresses are permitted by the any keyword, which means all hosts and is the equivalent of the wildcard mask 0.0.0.0 255.255.255.255. The allowed destination is indicated with the wildcard mask 0.0.0.255, which when used with the 192.168.144.0 network specifies the entire 192.168.144/24 subnet. Finally, the parameter eq 80 specifies that only HTTP traffic is allowed with this statement.

The command access-list 110 permit udp any 192.168.144.0 eq 80 is incorrect because a wildcard mask is not provided for the subnet. Also, HTTP uses TCP, not UDP.

The command access-list 10 permit tcp 192.168.144.0 255.255.255.0 eq www is incorrect because access list number 10 is in the range of a standard IP access lists and filters traffic on the basis of source IP address only. These access lists cannot permit or deny traffic for a destination network 192.168.144.0/24. Also, the mask is not in inverse or wildcard mask form. It should be entered as 0.0.0.255 instead of 255.255.255.0. The parameter eq www is acceptable, as you can use either the port number (80) or the service (www) with the eq parameter.

The command access-list 10 permit udp any 192.168.144.0 255.255.255.0 eq 80 is incorrect because the mask is not inverse or wildcard mask form. It should be entered as 0.0.0.255 instead of 255.255.255.0. Also, HTTP uses TCP, not UDP.

The command access-list 110 permit tcp 192.168.144.0 0.0.0.255 any eq 80 is incorrect because this statement would allow all traffic from the 192.168.144.0 subnet to access any destination using HTTP (port 80),

rather than permitting all traffic to HTTP servers in the 192.168.144.0/24 subnet.

The command access-list 110 permit tcp any 192.168.144.1 0.0.0.0 any eq 80 is incorrect because this statement would permit all traffic toa specific HTTP server with the IP address 192.168.144.1, rather than permitting all traffic to HTTP servers in the 192.168.144.0/24 subnet.

The command access-list 110 permit tcp any 192.168.144.1 0.0.0.255 any eq 23 is incorrect because this statement would permit all traffic using Telnet (port 23) to any server in the 192.168.144.0 subnet, rather than permitting all traffic to HTTP servers in the 192.168.144.0/24 subnet.

The command access-list 110 permit tcp 192.168.144.0 0.0.0.255 192.168.144.0 0.0.0.255 any eq 80 is incorrect because this statement would permit only traffic from computers in the 192.168.144.0 subnet using HTTP (port 80) to any server in the same subnet, rather than permitting all traffic to HTTP servers in the 192.168.144.0 subnet.

Several of the options are incorrect because of incorrect wildcard masks. When configuring the wildcard mask, a simple way to determine the correct wildcard mask is to look at the regular mask and subtract the value in the last octet from 255. That will give the proper wildcard mask value for that octet. For example, the proper wildcard mask for a 29-bit mask (or 255.255.255.248) would be 0.0.0.7 (255 - 248 = 7).

Another challenge that may arise is to deny a subnet that does not fall along classful lines.For example, your boss requires that you configure all hosts in the same subnet with the host at 172.16.5.118/26 to deny those hosts Telnet access to hosts outside the LAN. To arrive at the correct configuration, you must first determine the network ID ofthe network containing a computer that has an address of 172.16.5.118/26. With a /26 mask, the interval between subnets (and thus between network IDs) is 64. This creates the following sequence of network IDs:

172.16.0.64
172.16.0.128
172.16.0.192

and so on, until you arrive at the network ID of the network where this computer is located. The computer is in the 172.16.5.64 network because the next network ID in the series is 172.16.5.128. Because the wildcard mask is determined by viewing the regular mask (255.255.255.192) and subtracting the value in the regular mask's last octet from 255 (255 - 192 = 63), the wildcard mask is 0.0.0.63. Therefore, the following would be the proper access list line to configure this denial:

access-list 110 deny tcp 172.16.5.64. 0.0.0.63 any eq 23

The any parameter in the access list instructs the router that Telnet traffic should not be allowed to any IP addresses, since it is in the destination position in the command. If you wanted to block access to a single server at 192.168.5.1, for example, it would be replaced with the address of the server as follows:

access-list 110 deny tcp 172.16.5.64. 0.0.0.63 192.168.5.1 eq 23

To ensure that no other traffic types are affected by this list (as is usually the case), you must include a second line that specifically allows all other traffic. This is required because there is an implied deny all statement at the end of an access list, even if it uses permit statements. The full list would then appear this way:

access-list 110 deny tcp 172.16.5.64. 0.0.0.63 192.168.5.1 eq 23
access-list 110 permit any any

The any any section tells the router to permit traffic from any source to any destination.

Wildcard masks can also help to reduce the number of statements in an access list.Consider the following list of access list statements:

access-list 10 permit 172.168.16.0 0.0.0.255
access-list 10 permit 172.168.17.0 0.0.0.255
access-list 10 permit 172.168.18.0 0.0.0.255

access-list 10 permit 172.168.19.0 0.0.0.255

This will permit access to four subnets of the 172.168.0.0 class B network. But by using the correct wildcard mask applied to the first network in the series, you can specify the four subnets in a group with a single statement. To determine the correct mask, subtract the lowest network number from the highest to get the "width" of the group (19 - 16 = 3). Place that value in the third octet. Since the value in the last octet doesn't matter, place a 255 in that octet. This results in the wildcard mask of 0.0.3.255. Using this mask with the first network in the series allows you to replace the four statements with a single statement, as shown below:

access-list 10 permit 172.168.16.0 0.0.3.255

Objective:
Infrastructure Services

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

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

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

QUESTION 12
Which of the following accurately describes the purpose of a trunk?

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

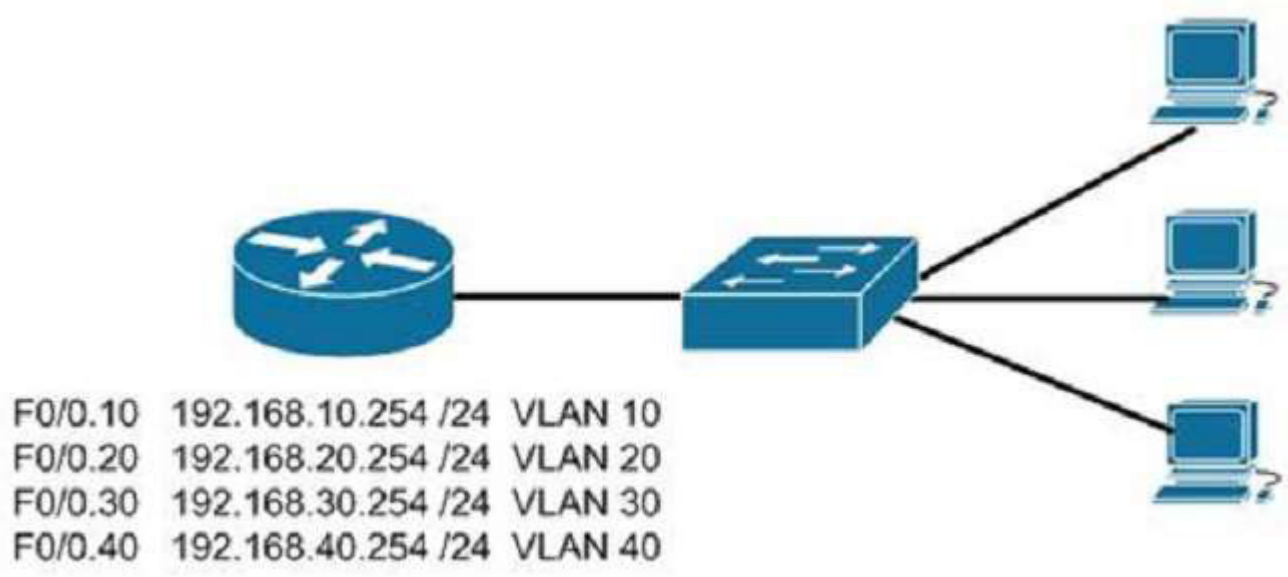
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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



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

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

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

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

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

QUESTION 13
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 isincorrect because 100VG-AnyLan uses demand priority as the access method.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Interpret Ethernet frame format

References:
http://docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols#LAN_Media-Access_Methods

QUESTION 14
You are the senior network administrator for a large corporation. Some new trainees have recently joined the network security team. You are educating them about denial-of-service (DoS) attacks and the risks posed to a network by such attacks.

Which three are risks that a DoS attack poses to a network? (Choose three.)

A. Downtime and productivity loss
B. Spread of viruses
C. Revenue loss
D. Information theft
E. Spread of spyware

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A DoS attack can result in network downtime and loss of productivity, revenue loss, and information theft.

A DoS attack is an attack in which legitimate users are denied access to networks, systems, or resources. The potential risks posed by a DoS attack are as follows:

- Downtime and productivity loss: A DoS attack causes downtime in the network, which ultimately results in loss of productivity for the organization.
- Revenue loss: Organizations that use their Web sites for commerce or vital support services, such as search

engines, can incur large revenue losses.
- Information theft: DoS attacks can also be aimed at stealing important and confidential information from a network.
- Malicious competition: An organization might launch DoS attacks against their competitors to damage their reputation.

A few methods that can help minimize potential risks from DoS attacks are:

- Using a firewall, which allows you to block or permit traffic entering into the network, can help to mitigate DoS attacks.
- Computers vulnerable to attacks can be shifted to another location or a more secure LAN.
- Intrusion Detection Systems (IDS), such as Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS), can be implemented to detect intrusive network or host activity, such as a DoS attack, and raise alerts when any such activity is detected.

A DoS attack does not result in the spread of viruses because viruses are not spread by DoS attacks. Viruses are spread when the network is attacked by a virus or a Trojan horse.

A DoS attack does not result in the spread of spyware. DoS attacks are mainly aimed at exhausting system resources so that legitimate users are denied access to networks, systems, or resources. Spyware is software installed on a computer without the knowledge of the user, and it gathers information about a person or organization. Spyware is generally downloaded through Web sites and e-mail messages.

Objective:
Infrastructure Maintenance

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

References:
https://www.cisco.com/c/en/us/td/docs/ios/sec_data_plane/configuration/guide/convert/sec_data_dos_atprvn_15_1_book/sec_cfg_tcp_intercpt.html#wp1000871

QUESTION 15

```
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:
https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_m1.html#wp1013837

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

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

QUESTION 16
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:

- Thedecimal 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:

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

QUESTION 17
Router-A# show running-configuration s0/0
interface serial0/0
description connected to router A
IP address 10.10.10.1 255.0.0.0
encapsulation frame-relay
shutdown
clock rate 64000

Based on the interface configuration provided, which two statements are TRUE? (Choose two.)

A. The router's serial interface is connected using a DTE cable.
B. The router's serial interface is connected using a DCE cable.
C. The router's serial interface is administratively down.
D. The router's serial interface connects using the point-to-point protocol.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The command output shows that the router's serial interface is connected to a DCE cable, and the router's serial 0/0 interface is administratively down. The clock rate is only configured when a DCE cable is connected to the router. Use the clock rate interface configuration command to configure the clock rate for the WAN link on serial interfaces. This command is used to set the interfaces clock rate to match the circuit clock rate.

This will only be the case when a router is connected to another router with a back-to-back serial cable.

Typically, a CSU/DSU acts as the DCE device and the router acts in a DTE role. The CSU/DSU terminates the digital local loop. In the case of an analog local loop, a modem would terminate the loop.

The command output proves that the router's serial 0/0 interface is administratively down by the presence of the shutdown statement for the serial 0/0 interface.

The router's serial interface does NOT connect to the CSU/DSU using a DTE cable. The clock rate statement would not be present when the serial interface is attached to a DTE cable.

The router's serial interface does NOT connect using the point-to-point protocol. The router is using the frame relay Layer 2 protocol as indicated by the encapsulation frame-relay statement in the output.

DTE and DCE serial cables can also be used to connect routers to each other. When a router connects to a CSU/DSU, it must use a DTE cable to connect. When two routers are connected, the router that supplies the clocking should be connected to the DCE cable. The other router should be connected to the DTE cable. The two cables are then connected to each other.

Objective:
Network Fundamentals

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

References:

QUESTION 18
Yesterday one of your associates made some changes to the syslog configuration on the router R69. Today, while working on the router you received this syslog message:

000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

Based on this output, which of the following commands did the associate execute?

A. service sequence-numbers
B. service timestamps log
C. service timestamps log datetime msec
D. logging console 4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The associate must have executed the service sequence-numbers command during his changes. This command instructs the syslog system to add a sequence number to each message, which can help to organize a timeline when messages are sent to a syslog server from various sources.

The associate could not have executed the service timestamps log command. This command enables time stamps on log messages, showing the time since the system was rebooted. If this had been done, a time stamp similar to the following would have been added to the message:

* Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

The associate could not have executed the service timestamps log date time msec command. This command enables time stamps on log messages, showing the time since the system was rebooted in milliseconds. If this had been done, a time stamp similar to the following would have been added to the message:

* Mar 1 18:46:11:058 %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

The associate could not have executed the logging console 4 command. This command instructs the syslog system to only display messages of levels 4, 3, 2 and 1 in severity. Since the message displayed is a level 5 message, this command could not have been executed.

Objective:
Infrastructure Maintenance

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

References:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-7-0E/15-23E/configuration/guide/xe-370-configuration/log.html#71808

QUESTION 19
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.

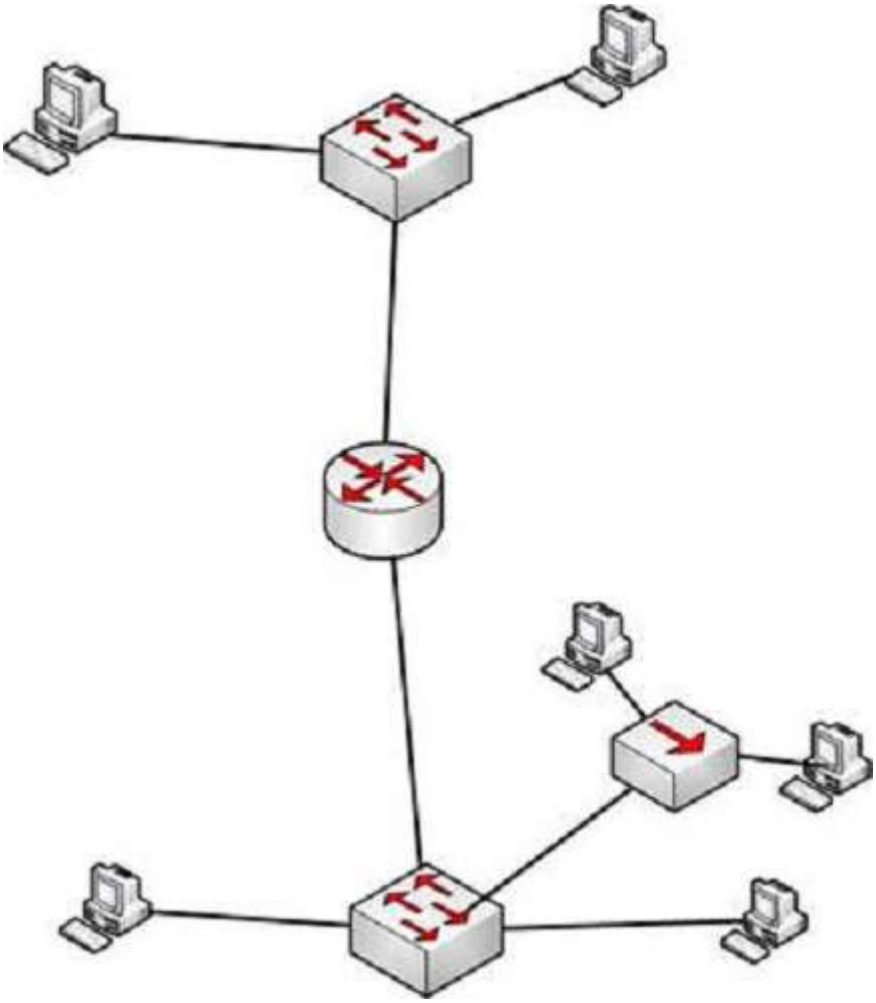
Objective:
Routing Fundamentals

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

References:
http://www.omnisecu.com/cisco-certified-network-associate-ccna/difference-between-ripv1-and-ripv2.php

http://www.ciscopress.com/articles/article.asp?p=102174

QUESTION 20
How many collision and broadcast domains are in the network shown below?

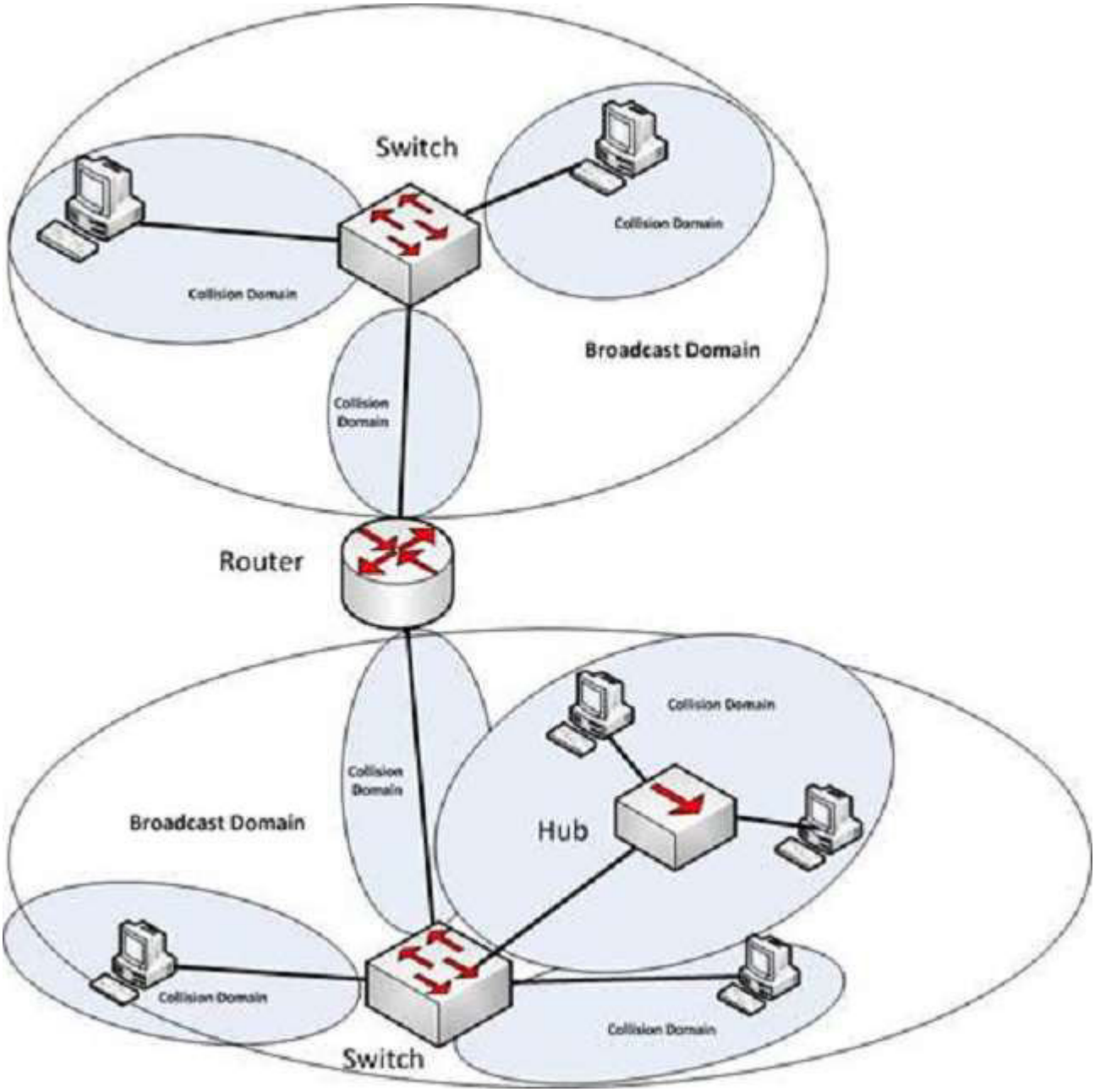


A. 4 collision domains and 3 broadcast domains
B. 7 collision domains and 2 broadcast domains
C. 8 collision domains and 1 broadcast domain
D. 6 collision domains and 2 broadcast domains

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

QUESTION 21
Which statements are NOT true regarding Virtual Local Area Networks (VLANs)? (Choose two.)

A. VLANs define broadcast domains.
B. VLANs are logical groups of hosts.

C. VLANsare location-dependent.
D. VLANs are limited to a single switch.
E. VLANs may be subnets of major networks.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

VLANs are NOT location-dependent and can span to multiple switches using trunk links. VLANs provide location independence that makes addition, change, and movement of networking devices a simple process. VLANs allow you to group people according to their job function, which also eases the implementation of security policies.

A VLAN is a group of networking devices in the same broadcast domain. Each time you create a new VLAN on a switch, a new broadcast domain is created. VLANs are not restricted to any physical boundary in the switched network. VLANs operate as separate subnets, and so for inter-VLAN communication to occur there must be a router in the network or a route feature card in one of the switches. In other words, if a switch is configured with two VLANs, and there are hosts connected to the VLANs, then hosts in one VLAN will be unable to connect to hosts in another VLAN if the switch is not connected to a router.

VLANs are logical groups of hosts. A host or user can be located anywhere in the switched network and still belong to the same broadcast domain. If you move a host from one switch to another switch in the same switched network, you can still keep the host in the original VLAN.

VLANs may be subnets of a major network. A subnet is a contained broadcast domain. A broadcast that occurs in one subnet will not be forwarded, by default, to another subnet. Layer 3 devices provide the forwarding function at boundary. Each of these subnets requires a unique network number. To move from one network number to another, you need a Layer 3 device. Each VLAN is a separate broadcast domain and requires a Layer 3 device for inter-VLAN routing.

Securing access to sensitive devices can be achieved in two steps:

- Access lists enforced at the router
- Restricted VLANs configured on the switches

From a security standpoint, devices can be placed on a private VLAN to prevent sensitive information from being captured by devices on other VLANs. Access lists enforced at the router can be used to prevent unauthorized access to the private VLAN.

VLANs provide the following benefits:

- Logical, rather than physical, grouping of devices
- Grouping of devices by function or department
- Enhanced network security
- Decreased size of broadcast domains with the increased number of broadcast domains
- VLAN greatly simplify adding, moving and changing host in the network

VLANs have the following characteristics

- VLANs logically divide a switch into multiple, independent switches at Layer 2
- A VLAN can span multiple switches
- Trunk links can carry traffic for multiple VLANs between the switches and between the switch and a router
- VLAN create segmented broadcast domains in switched networks

Objective:
LAN Switching Fundamentals

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

References:

https://www.cisco.com/c/en/us/products/collateral/routers/1700-series-modular-access-routers/prod_end-of-life_notice0900aecd8044473f.html

QUESTION 22
The following access list has been applied to an interface on a router:

access-list 101 deny tcp 192.111.16.32 0.0.0.31 host 192.168.5.60

Disregarding the implicit deny at the end of the list, which of the following IP addresses will be blocked because of this single rule in the list? (Choose all that apply.)

A. 192.111.16.67
B. 192.111.16.38
C. 192.168.5.60
D. 192.111.16.49
E. 192.168.111.14

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The access list will block the addresses 192.111.16.38 and 192.111.16.49. The scope of an access list is determined by the wildcard mask and the network address to which it is applied. Use the value in the wildcard mask and increment the network address in the same octet as the value of the mask to determine the scope of the list.

For example, in this case the starting point of the list of addresses affected by the mask is the network ID 192.111.16.32. The wildcard mask is 0.0.0.31. Adding the value of the last octet in the mask to the network address (32 + 31 = 63) tells you where the effects of the access list ends, which is 192.111.16.63. Therefore, all addresses in the range 192.111.16.32 - 192.111.16.63 will be denied by this list.

None of the other IP addresses falls into this range.

This process works the same in other octets as well. For example, consider this list:

access-list 101 deny tcp 192.111.16.0 0.0.15.255 host 192.168.5.60

When a wildcard mask has 255 in an octet, as in the last octet of this wildcard mask, then any address will match the list in that octet. In this case, we use the value in the octet to the left of the 255 octet to determine the scope of the list. The procedure is the same as the first example. The starting point is the network address, which is 192.111.16.0. The wildcard mask is 0.0.15.255. Adding the value of the third octet in the mask to the network address (16 + 15 = 31) shows where the effects of the access list ends, which is 192.111.31.255. Therefore, all addresses in the range 192.111.16.1 - 192.111.31.255 will be denied by this list.

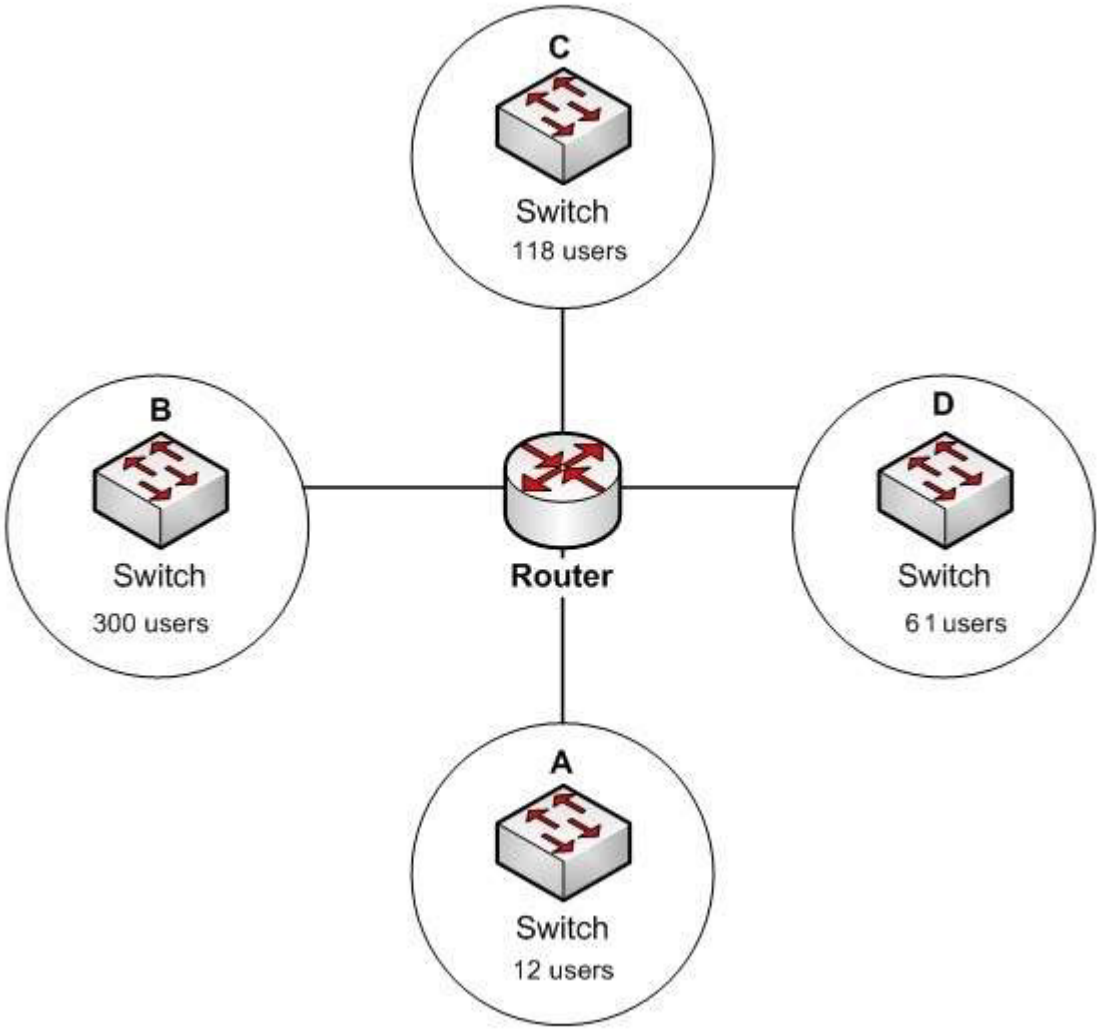
Objective:
Infrastructure Services

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

References:

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

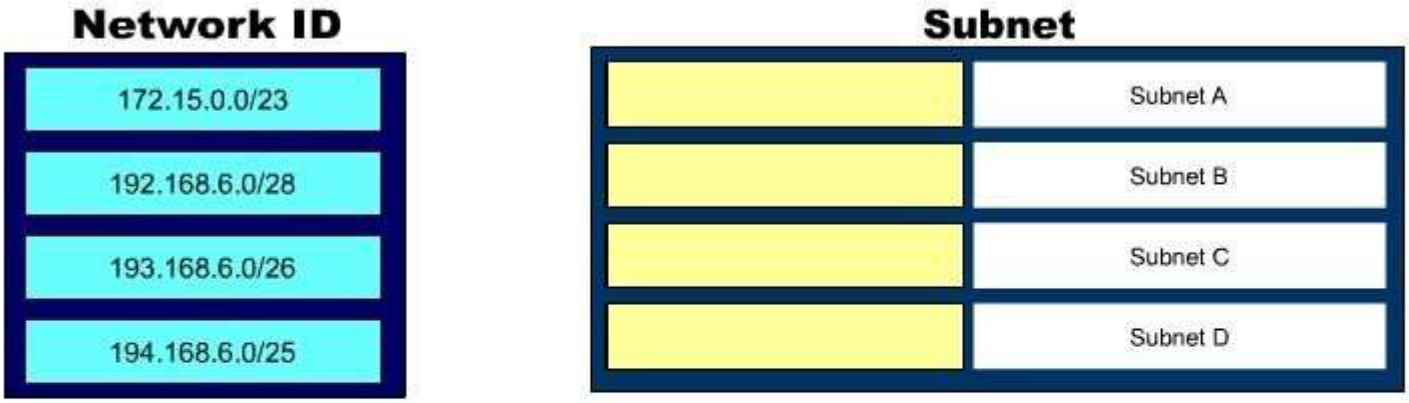
QUESTION 23
DRAG DROP
Click the Exhibits button at the bottom of the page to examine a proposed network diagram. There are four proposed subnets, labeled A, B, C, and D. Subnet A will have 12 users, subnet B will have 300 users, subnet C will have 118 users, and subnet D will have 61 users.



You are designing the IP addressing for this network. You are instructed not to waste IP addresses by making the subnets larger than necessary. Click and drag the correct network ID from the left to the appropriate subnet on the right.

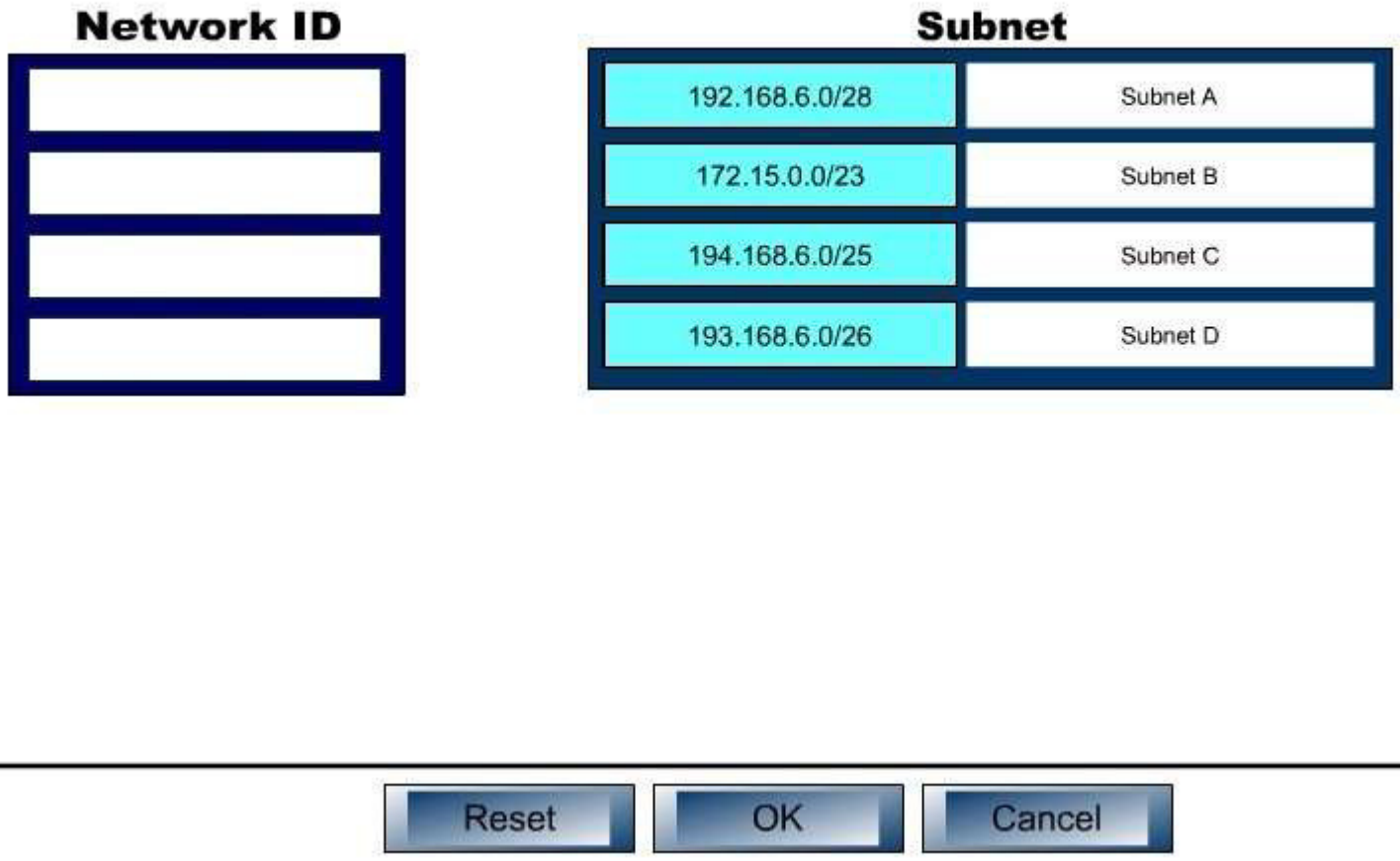
Select and Place:

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



Correct Answer:

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



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Subnet A needs to support 12 users. The number of possible addresses in a subnet is determined by the number of host bits or zeros in the mask. The formula is 2n -2 , where n is the number of host bits. Therefore, to support 12 users efficiently, the subnet mask requires no more and no less than four host bits. When there are four host bits in the mask there 28 bits in the network portion. That is the case with 192.168.6.0/28.

Subnet B needs to support 300 users. To support 300 users without wasting addresses, the mask requires no more and no less than nine host bits. When there nine host bits in the mask, there are 23 bits in the network portion. That is the case with 172.15.0.0/23.

Subnet C needs to support 118 users. To support 118 users without wasting addresses, the mask requires no more and no less than seven host bits. When there seven host bits in the mask, there are 25 bits in the network portion. That is the case with 194.168.6.0/25.

Subnet D needs to support 61 users. To support 61 users without wasting addresses, the mask requires no more and no less than six host bits. When there six host bits in the mask, there are 26 bits in the network portion. That is the case with 193.168.6.0/26.

Objective:
Network Fundamentals

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

References:

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

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

QUESTION 24
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 cdpadvertise-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:

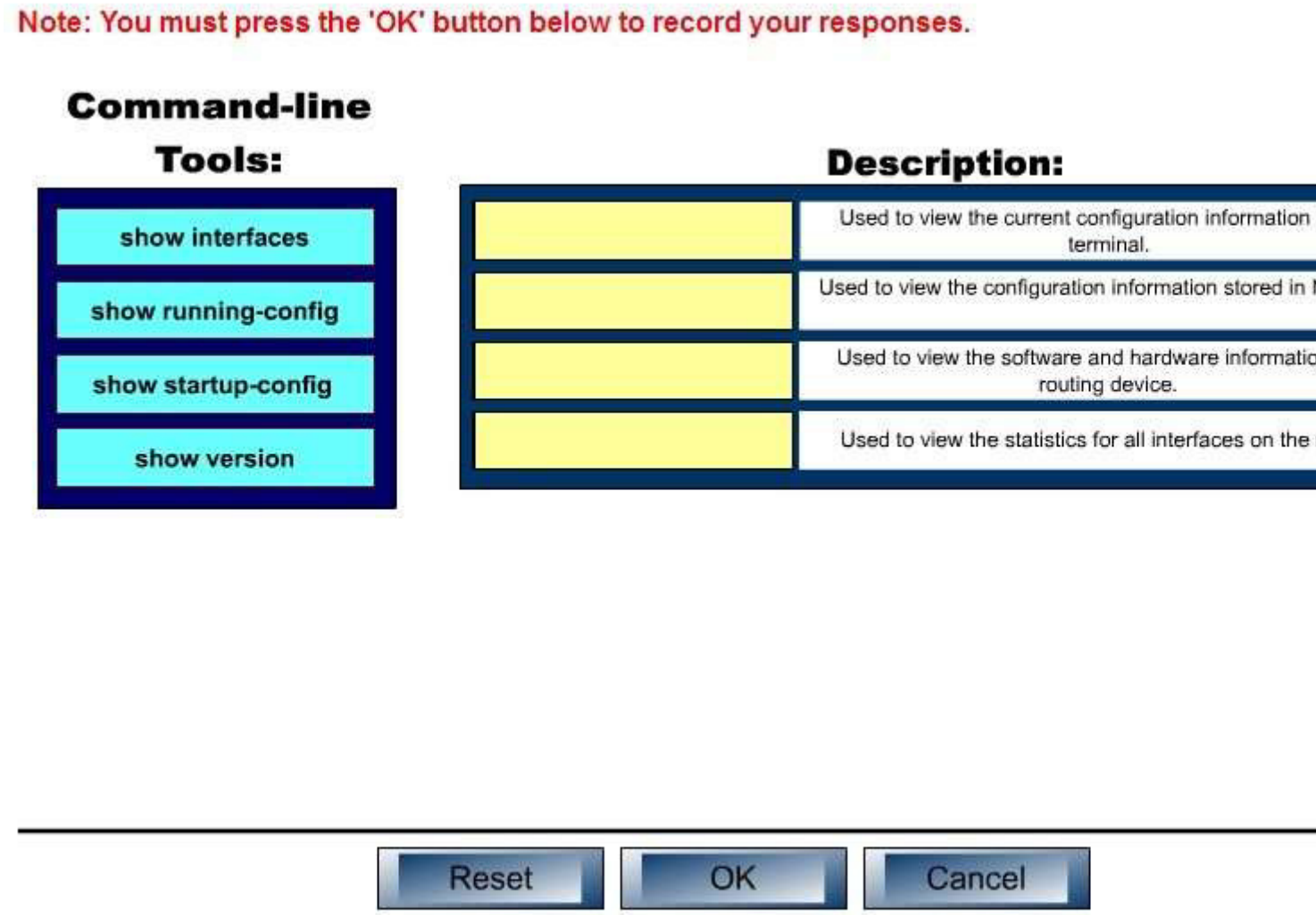
https://search.cisco.com/search?query=Cisco%20IOS%20Network%20Management%20Configuration%20Guide&locale=enUS&tab=Cisco

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

https://www.cisco.com/en/US/tech/tk962/technologies_security_notice09186a0080093ef0.html#summary

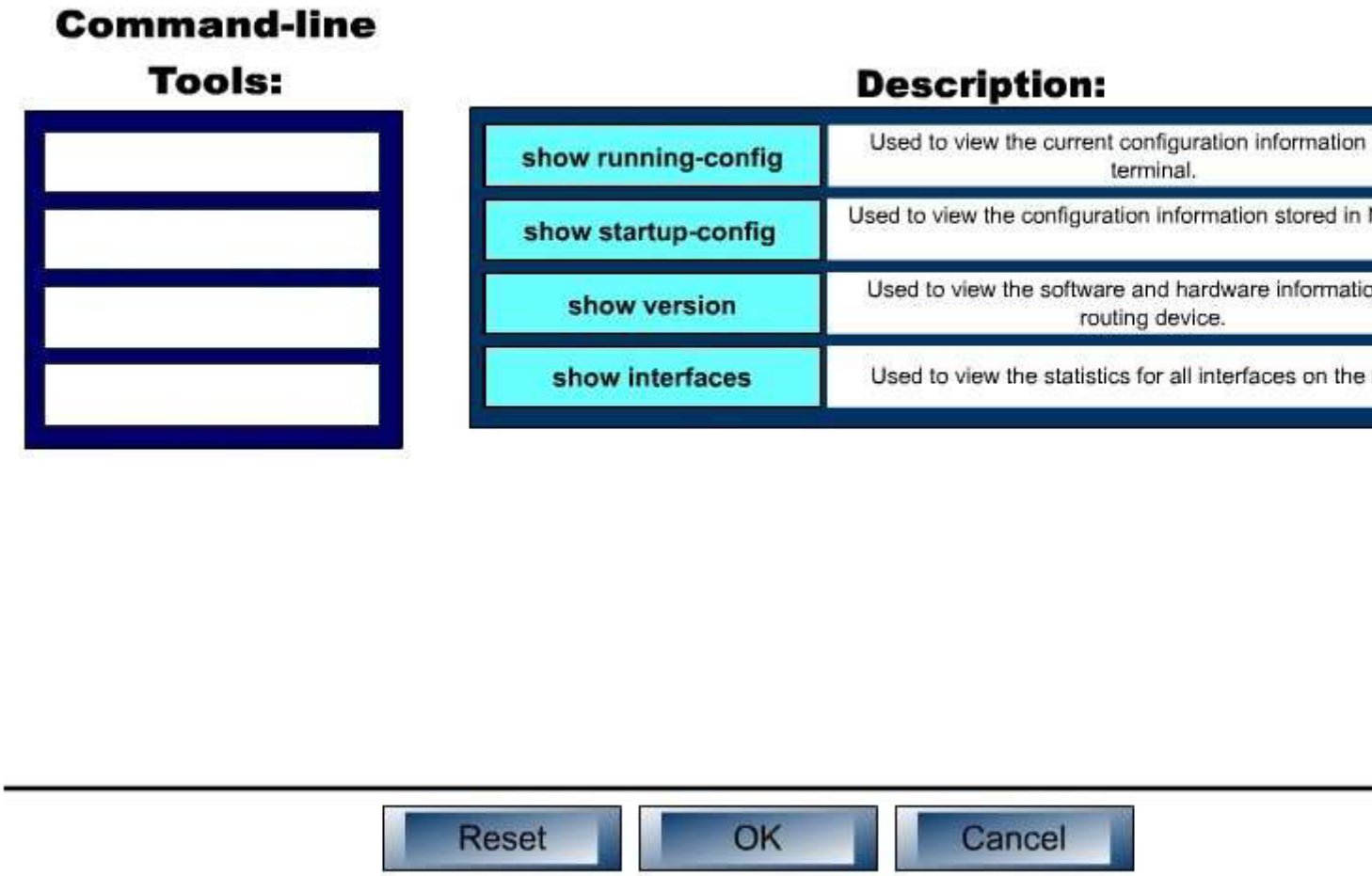
QUESTION 25
DRAG DROP
Click and drag the show commands on the left to their appropriate description on the right.

Select and Place:



Correct Answer:

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



Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show commands and their appropriate descriptions are as follows:

- show interfaces: Used to view configured interfaces on the router.
- show running-config: Used to view the currently running configuration.
- show startup-config : Used to view the stored configuration in router's NVRAM.
- show version: Used to view configuration of system hardware, software version, and boot images.

The following commands are also used to view the information on the router:

- show controllers: Used to view interface card controllers.
- show flash: Used to view contents of flash memory.
- show process cpu: Used to view active processes on the router.
- show debugging: Used to view which type of debugging is enabled on the router.

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

References:
https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_s2.html#wp1444377

QUESTION 26
What data structure is pictured in the graphic?

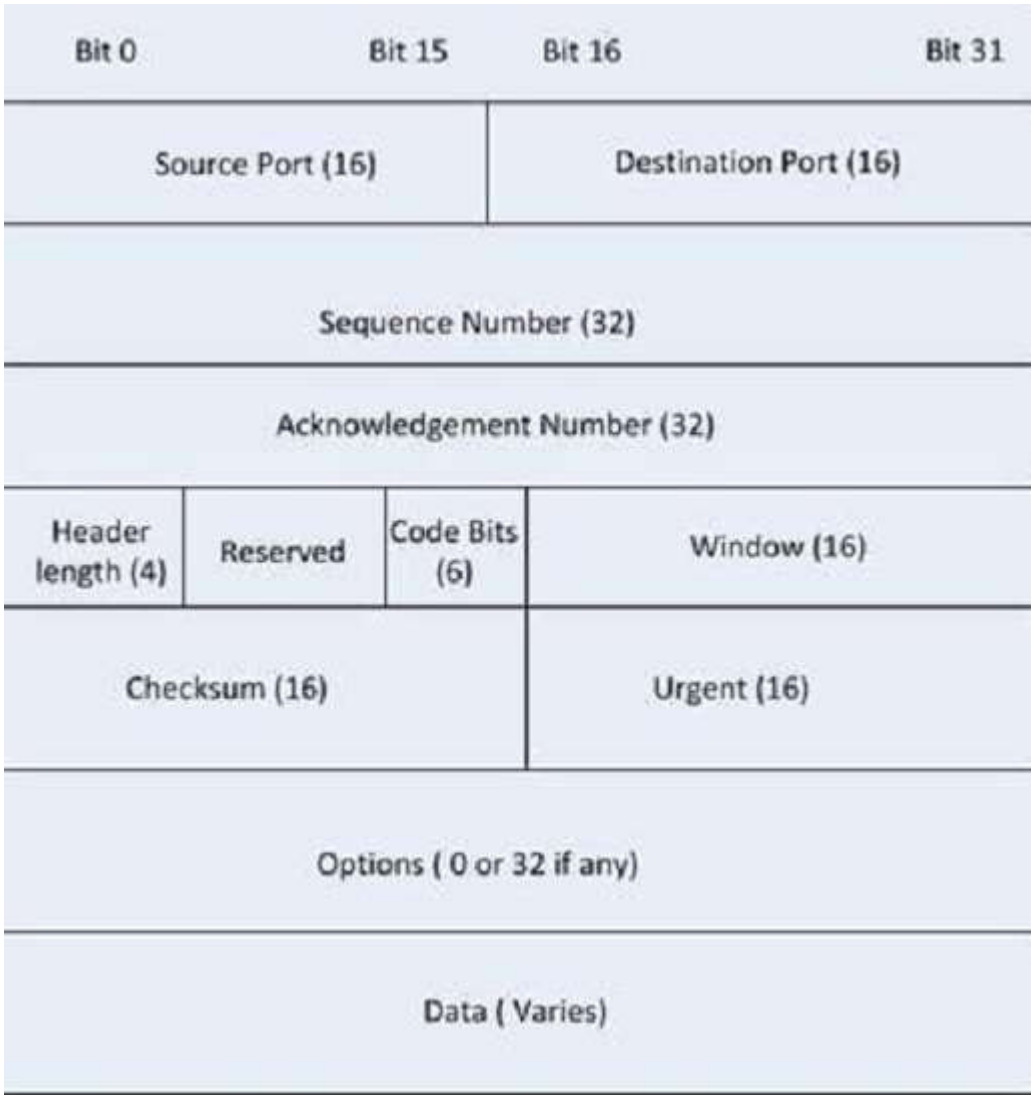
A. TCP segment
B. UDP datagram
C. IP header
D. Http header

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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



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

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

Objective:
Network Fundamentals

Sub-Objective:
Compare and contrast TCP and UDP protocols

References:

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

QUESTION 27
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:

https://search.cisco.com/search?query=Cisco%20IOS%20Network%20Management%20Configuration%20Guide&locale=enUS&tab=Cisco

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

https://www.cisco.com/en/US/tech/tk962/technologies_security_notice09186a0080093ef0.html#summary

QUESTION 28
Which of the following statements are TRUE regarding Cisco access lists? (Choose two.)

A. In an inbound access list, packets are filtered as they enter an interface.
B. In an inbound access list, packets are filtered before they exit an interface.
C. Extended access lists are used to filter protocol-specific packets.
D. You must specify a deny statement at the end of each access list to filter unwanted traffic.
E. When a line is added to an existing access list, it is inserted at the beginning of the access list.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

In an inbound access list, packets are filtered as they enter an interface. Extended access lists are used to filter protocol specific packets. Access lists can be used in a variety of situations when the router needs to be given guidelines for decision-making. These situations include:

-Filtering traffic as it passes through the router
- To control access to the VTY lines (Telnet)
- To identify "interesting" traffic to invoke Demand Dial Routing (DDR) calls
- To filter and control routing updates from one router to another

There are two types of access lists, standard and extended. Standard access lists are applied as close to the destination as possible (outbound), and can only base their filtering criteria on the source IP address. The number used while creating an access list specifies the type of access list created. The range used for standard access lists is 1 to 99 and 1300 to 1999. Extended access lists are applied as close to the source as possible (inbound), and can base their filtering criteria on the source or destination IP address, or on the specific protocol being used. The range used for extended access lists is 100 to 199 and 2000 to 2699.

Other features of access lists include:

- Inbound access lists are processed before the packet is routed.
- Outbound access lists are processed after the packet has been routed to an exit interface.
- An "implicit deny" is at the bottom of every access list, which means that if a packet has not matched any preceding access list condition, it will be filtered (dropped).
- Access lists require at least one permit statement, or all packets will be filtered (dropped).
- One access list may be configured per direction for each Layer 3 protocol configured on an interface

The option stating that in an inbound access list, packets are filtered before they exit an interface is incorrect. Packets are filtered as they exit an interface when using an outbound access list.

The option stating that a deny statement must be specified at the end of each access list in order to filter unwanted traffic is incorrect. There is an implicit deny at the bottom of every access list.

When a line is added to an existing access list, it is not inserted at the beginning of the access list. It is inserted at the end. This should be taken into consideration. For example, given the following access list, executing the command access-list 110 deny tcp 192.168.5.0 0.0.0.255 any eq www would have NO effect on the packets being filtered because it would be inserted at the end of the list, AFTER the line that allows all traffic.

access-list 110 permit ip host 192.168.5.1 any
access-list 110 deny icmp 192.168.5.0 0.0.0.255 any echo
access-list 110 permit any any

Objective:
Infrastructure Services

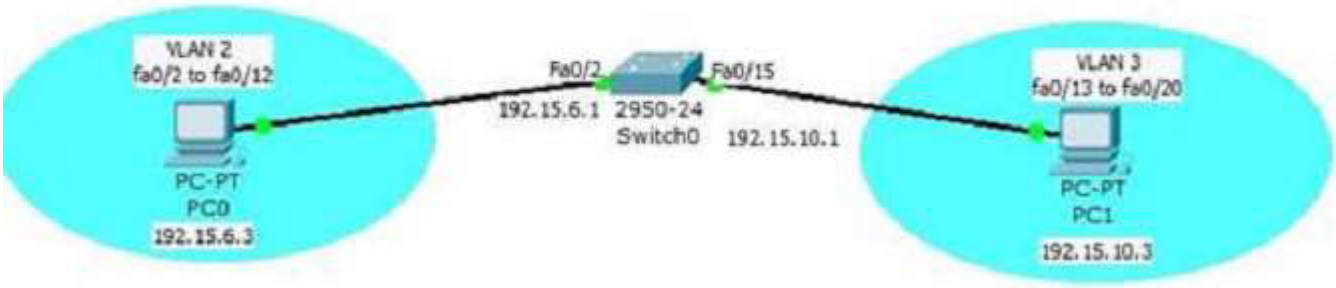
Sub-Objective:
Configure, verify, and troubleshoot IPv4 standard numbered and named access list for routed interfaces

References:

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

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

QUESTION 29
The following exhibit displays ALL devices currently connected to Switch0:



Which of the following statements is true of this scenario?

A. PC0 can communicate with PC1
B. If we change the IP address of PC1 to 192.168.6.4, PC1 will be able to connect with PC0
C. If we change the VLAN of Fa0/15 to VLAN 2, PC0 will be able to connect with PC1
D. If we change the VLAN of Fa0/2 to VLAN 3 and change the IP address of PC1 to 192.168.6.5, PC1 will be able to connect with PC0

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

If we change the VLAN of Fa0/2 to VLAN 3 and change the IP address of PC1 to 192.168.6.5, PC0 will be able to connect with PC1. In the configuration shown in the diagram, the two PCs are connected to interfaces in different VLANs and have IP addresses in different IP subnets. That is the normal configuration when creating VLANs. In the current configuration, PC0 cannot communicate with PC1 because there is no router in the scenario to route between the VLANs. However, if we place both interfaces in the same VLAN and place both PCs in the same IP subnet, no router will be required for the PCs to communicate.

If we change the IP address of PC1 to 192.168.6.4, it will still not be able to connect with PC0 because they will still be in different VLANs. They must be in both the same VLAN and the same IP subnet to communicate in the absence of a router to route between VLANs.

If we change the VLAN of Fa0/15 to VLAN 2, PC0 will still not be able to connect with PC1 because they will still be in different IP subnets. They must be in both the same VLAN and the same IP subnet to communicate in the absence of a router to route between VLANs.

Objective:
Routing Fundamentals

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

References:
http://www.ciscopress.com/articles/article.asp?p=2104949

https://community.spiceworks.com/how_to/55605-how-to-configure-router-on-a-stick

QUESTION 30
Which trunk encapsulation defines one VLAN on each trunk as a native VLAN?

A. ISL
B. IEEE 802.1q
C. IEEE 802.11a
D. auto

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

IEEE 802.1q defines one VLAN on each trunk as the native VLAN.

The default value of a native VLAN is VLAN1. The IEEE 802.1q method does not encapsulate frames when forwarded over a trunk in a native VLAN; that is, IEEE 802.1q does not add its header information while transmitting frames in the native VLAN. This traffic is called untagged traffic. .Frames originating from other VLANs, however, will have a 4-byte 802.1q header inserted into the frame to identify the VLAN number.

The native VLAN number can be changed if desired. If done it should be done on both ends of the connection. Otherwise, traffic that uses the native VLAN (untagged traffic) will not be able to cross the link. The commend to change the native VLAN is

Switch(config)#switchport trunk native vlan vlan number

Inter Switch Link (ISL) does not define one VLAN on each trunk as a native VLAN. ISL is the Cisco proprietary trunk encapsulation, and it can only be used between two Cisco switches.

IEEE 802.11a is a wireless standard defined by the IEEE, and has nothing to do with VLANs.

Auto is not an encapsulation method. The auto trunking mode is a method for negotiating an encapsulation method over trunk links.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure and verify Layer 2 protocols

References:

https://www.cisco.com/c/en/us/support/docs/wireless/aironet-1100-series/46141-vlanswireless.html

QUESTION 31
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 becausea router does not store the IOS image in NVRAM. The startup configuration is stored in NVRAM.

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15-s/fundamentals-15-s-book.html#wp1001809

QUESTION 32
A packet is received with a destination IP address of 10.2.16.10. What would the next hop IP address be for this packet?

Router# show ip route
<<output omitted>>

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

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

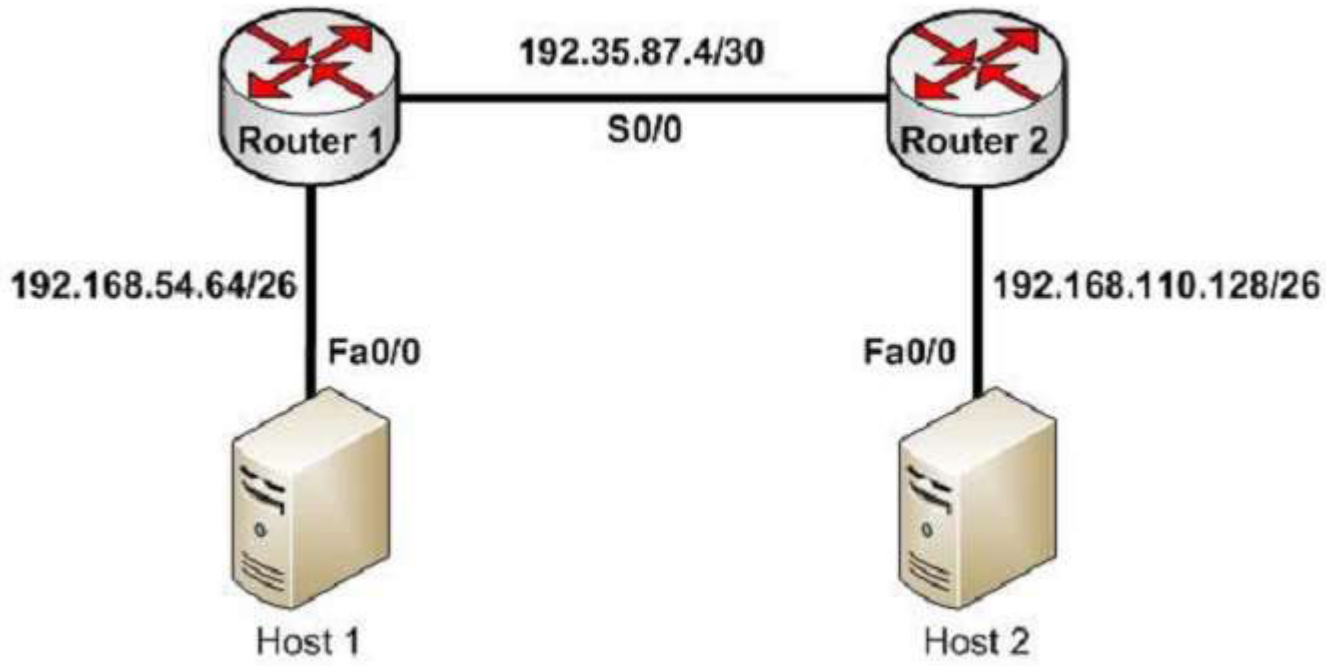
The packet will not be dropped because there is at least one routing table entry that matches the destination IP address of the packet.

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

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

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

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



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

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

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

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

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

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

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

References:

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

QUESTION 33

You have discovered that Router 8 on your network is not receiving updates from Router 10. Router10 has an IP address of 201.56.41.9. All routers run RIP. Since you are new and not completely familiar with the topology of the network, you execute the debug ip rip command on Router 8 and receive the results shown below:

Router8# debug ip rip
*Mar 1 07:35:12.070: RIP: sending v2 update to 201.56.41.9 via Serial0/0 (201.56.41.88)
*Mar 1 07:35:12.074: RIP: build update entries
*Mar 1 07:35:19.638: RIP: ignored v2 packet from 201.56.41.9 (invalid authentication)

What can be the problem? (Choose all that apply.)

A. Router 10 has not yet been configured for authentication
B. Router 10 is configured for RIPv2 and Router 8 is configured for RIP v1.
C. There is a connectivity problem between the routers.
D. Router 10 is over 16 hops away
E. The password is not correct.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The problem can be that Router 10 has not yet been configured for authentication or that the password is not correct. This can be ascertained by the line in the debug output shown below:

*Mar 1 07:35:19.638: RIP: ignored v2 packet from 201.56.41.9 (invalid authentication)

It is not a problem with RIP version mismatch. If that were the problem, the following statement would be a line in the output:

*Mar 1 07:35:19.638: RIP: ignored v2 packet from 201.56.41.9 (illegal version)

It is not a connectivity problem. If there were a connectivity problem, we would not be receiving an attempt at an update from Router 10.

Router 10 is not more than 16 hops away. If that were the case, that information would be received from another router in its updates as shown below:

*Mar 1 07:35:19.638: RIP: received update from 201.56.41.10 via Serial0/0
201.56.41.9 in 16 hops (inaccessible)

Objective:
Routing Fundamentals

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

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

QUESTION 34
In what order are the lines of an access list read when an access list is applied to a router interface? (Choose all that apply.)

A. Top to bottom if it is a standard access list

B. Top to bottom it is an extended access list
C. Bottom to top, if it is a standard access list
D. Bottom to top, if it is an extended access list

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Extended access lists, just as standard access lists, are read from top to bottom. Therefore, when creating access lists, you want to create the more specific statements and the more frequently occurring conditions towards the top of the list and the more general statements towards the end. When a deny statement is encountered, all statements that follow in the list that apply to the same type of traffic on that interface are ignored.

There are two types of access lists, standard and extended. Extended access lists can be either named or numbered. Characteristics of named access lists include:

- Individual statements within the list can be deleted, rather than deleting the entire list as is required with numbered lists.
- Named lists must specify whether they are standard or extended. With numbered lists, this is indicated by the use of specific list number ranges.
- The ip access-list command is used for numbered lists rather than the access-list command as is used with numbered lists.

Standard access lists are applied as close to the destination as possible (outbound), and can only base their filtering criteria on the source IP address. The number used while creating an access list specifies the type of access list created. The range used for standard access lists is 1 to 99 and 1300 to 1999.

Extended access lists are applied as close to the source as possible (inbound), and can base their filtering criteria on the source or destination IP address, or on the specific protocol being used. The range used for extended access lists is 100 to 199 and 2000 to 2699.

Access lists express the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router or packets that exit outbound interfaces of the router. Access lists do not act on packets that originate from the router itself. Instead, access lists are statements that specify conditions on how the router will handle the traffic flowing through specified interfaces.

The other options are incorrect because access lists are always read from top to bottom.

Objective:
Infrastructure Services

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

References:

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

QUESTION 35
Which type of switching process requires a switch to wait for the entire frame to be received before forwarding it to a destination port?

A. store and forward
B. cut-through

C. fragment free
D. frame-forward

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The store and forward switching process requires a switch to wait until the entire frame is received before forwarding it to a destination port. The store and forward method increases latency as it buffers the entire frame and runs a Frame Check Sequence (FCS) before forwarding it to destination port. However, it ensures error-free frame forwarding because its filters all frame errors.

The cut-through switching process does NOT require a switch to verify the FCS in a frame before forwarding it to the destination port. This type of internal switching method is faster than the store and forward process, but may forward error frames.

The fragment-free switching process only waits to receive the first 64 bytes of the frame before forwarding it the destination port. Fragment-free internal switching assumes that if there is no error in the first 64 bytes of the data, the frame is error free. The assumption is based on the fact that if a frame suffers a collision, it occurs within the first 64 bytes of data. Fragment-free forwarding speed lies between that of store and forward and cut-through.

The term frame-forward is not a valid internal switching process for Cisco switches.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

References:

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

QUESTION 36
Which of the following commands will configure a router to use DNS for hostname resolution?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

Objective:
Infrastructure Services

Sub-Objective:
Describe DNS lookup operation

References:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/15-mt/dns-15-mt-book/dns-config-dns.html

QUESTION 37
In which two situations would it be appropriate to issue the ipconfig command with the /release and /renew options? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

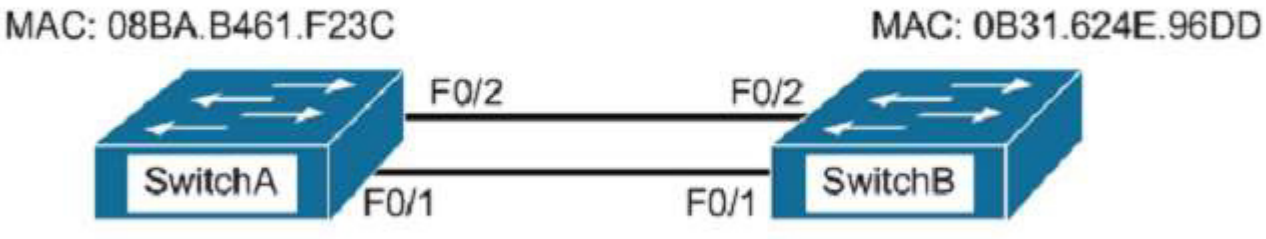
These commands also will be of no benefit if the no ip directed-broadcast command has been issued in the router interface local to the client and no IP helper address has been configured on the router between the client and the DHCP server. The no ip directed-broadcast command instructs the router to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

Objective:
Infrastructure Services

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

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

QUESTION 38
Which switch port will be in a blocking state? (Click the Exhibit(s) button to view the switch port diagram.)



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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

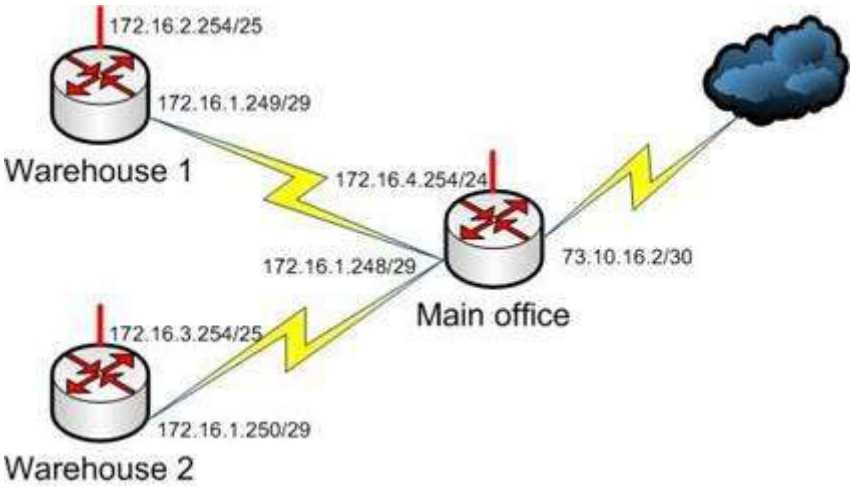
Objective:
LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

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

QUESTION 39
The router interfaces for a network are configured as shown in the following exhibit. (Click the Exhibit(s) button.)



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

What should you do to fix this problem?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

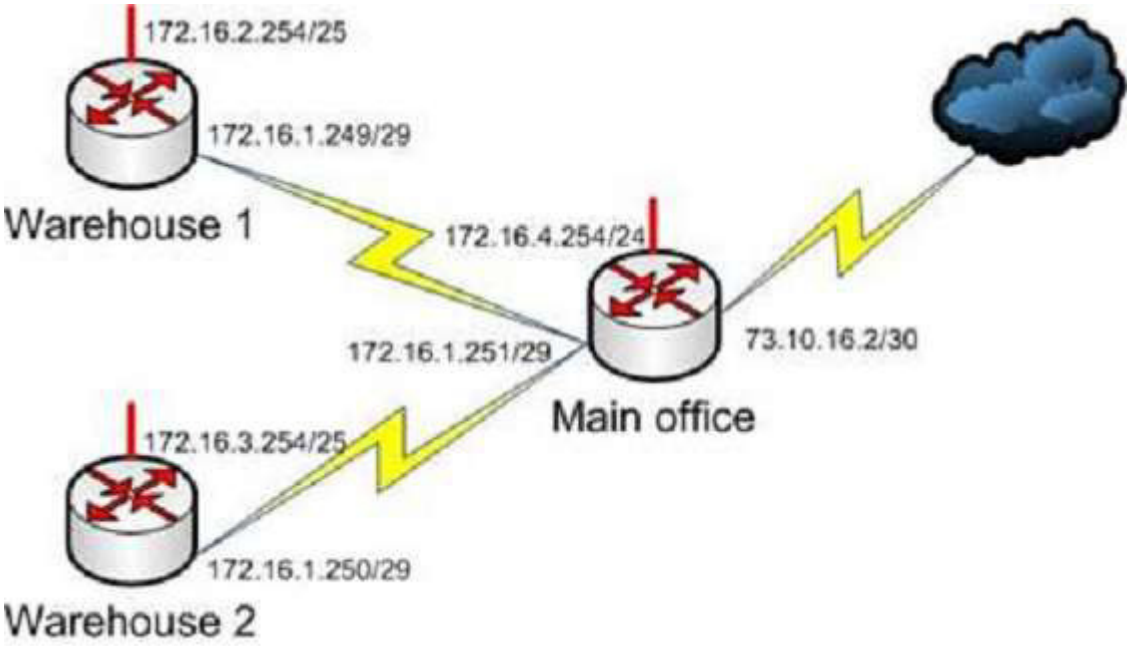
With a 29-bit mask and the chosen class B address,the following network IDs are created:

172.16.0.0
172.16.0.8
172.16.0.16
172.16.0.24
172.16.0.32
172.16.0.40
172.16.0.48
172.16.0.56
172.16.0.64
and so on, incrementing each time by 8 in the last octet. At the end of this series of increments, the network IDs will be:

172.16.1.240
172.16.1.248
172.16.2.0

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

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



Objective:
Network Fundamentals

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

References:

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

QUESTION 40
During the process of connecting four switches to the central router and implementing VLANS between the devices, it becomes apparent that there was a misunderstanding about which encapsulation protocol to use on the links between the switches and the router.

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

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

Objective:
LAN Switching Fundamentals

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

References:

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

QUESTION 41
Which command would be used to establish static translation between an inside local address 192.168.144.25 and an inside global address 202.56.63.102?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

ip nat inside source static local-ip global-ip

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

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

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

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

Objective:
Infrastructure Services

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

References:

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

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

QUESTION 42
Which of the following is NOT a VLAN Trunking Protocol (VTP) mode of operation?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

Objective:

LAN Switching Fundamentals

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

References:

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

QUESTION 43
Which Cisco IOS command is used to view the information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

The syntax of the command is as follows:

Router# show cdp interface [type number]

The parameters of the command are as follows:

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

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

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

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

NewYork#show interfaces s0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet Address is 192.168.10.1/24

MTU 1500 bytes,BW 1544 Kbit
Reliability 255/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)

LosAngeles#show interfaces s1
Serial0 is up, line protocol is up
Hardware is HD64570
Internet Address is 192.168.11.2/24
MTU 1500 bytes,BW 56000 Kbit
Reliability 255/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)

Notice that the following settings are correct:

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

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

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

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

Objective:
LAN Switching Fundamentals

Sub-Objective:
Configure and verify Layer 2 protocols

References:

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

QUESTION 44
Your assistant just entered the following command on a router:

R67(config)#logging trap 0

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

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

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

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

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

Objective:
Infrastructure Maintenance

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

References:

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

QUESTION 45
Which Cisco IOS Cisco Discovery Protocol (CDP) command displays the IP address of the directly connected Cisco devices?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

Tecumsah# show cdp neighbors detail

Device ID: Tacoma
Entry address(es):
IP address: 172.19.169.88
Platform: cisco 7206VXR, Capabilities: Router

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

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

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

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

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

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

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

Objective:
Infrastructure Maintenance

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

References:

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

QUESTION 46
At which layer in the Open Systems Interconnection (OSI) model does flow control generally operate?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

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

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

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

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

Objective:
Network Fundamentals

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

References:

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

QUESTION 47
Refer to the partial output of the show interfaces command:

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

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

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

Objective:
Infrastructure Maintenance

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

References:

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

QUESTION 48
A host is powered up, but the connected switch port does not turn amber or green. Which of the following methods would you use to troubleshoot the situation? (Choose three. Each answer is a complete solution.)

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

References:

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

QUESTION 49
Which two features do Cisco routers offer to mitigate distributed denial-of-service (DDoS) attacks? (Choose two.)

A. Anti-DDoS guard
B. Scatter tracing
C. Access control lists (ACLs)
D. Flow control
E. Rate limiting

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Cisco routers use access control lists (ACLs) and blackholing features to help mitigate distributed denial-of-service (DDoS) attacks. A DoS attack is an attack in which legitimate users are denied access to networks, systems, or resources. One of the most common DoS attacks is the DDoS attack, which is executed by using multiple hosts to flood the network or send requests to a resource. The difference between DoS and DDoS is that in a DoS attack, an attacker uses a single host to send multiple requests, whereas in DDoS attacks, multiple hosts are used to perform the same task.

Cisco routers offer the following features to mitigate DDoS attacks:

- ACLs: Filter unwanted traffic, such as traffic that spoofs company addresses or is aimed at Windows control ports. However, an ACL is not effective when network address translation (NAT) is implemented in the network.
- Rate limiting: Minimizes and controls the rate of bandwidth used by incoming traffic.
- Traffic-flow reporting: Creates a baseline for the network that is compared with the network traffic flow, helping you detect any intrusive network or host activity.
- Apart from these features offered by Cisco routers, the following methods can also be used to mitigate DDoS attacks:
- Using a firewall, you can block or permit traffic entering a network.
- The systems vulnerable to attacks can be shifted to another location or a more secure LAN.
- Intrusion Detection Systems (IDS), such as Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS), can be implemented to detect intrusive network or host activity such as a DoS attack, and raise alerts when any such activity is detected.

Anti-DDoS guard and scatter tracing are incorrect because these features are not offered by Cisco routers to mitigate DDoS attacks.

Flow control is incorrect because flow control is used to prevent the loss of traffic between two devices.

Objective:

Infrastructure Maintenance

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

References:

https://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.html

QUESTION 50
Which Cisco Internetwork Operating System (IOS) command is used to define an access list by name?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

The parameters of the command are as follows:

- standard: Specifies an standard IP access list.
- extended: Specifies an extended IP access list.
- access-list-name: Specifies the name of the access list.

The ip access list command is incorrect because this command does not exist in Cisco IOS terminology. The correct command syntax is ip access-list.

The ip access-group command is incorrect because this command is used to apply an access list to an interface.

The access-list command is incorrect because this command is used to create a numbered access control list entry.

Objective:
Infrastructure Services

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

References:

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

QUESTION 51
You need to manually assign IPv6 addresses to the interfaces on an IPv6-enabled router. While assigning addresses, you need to ensure that the addresses participate in neighbor discovery and in stateless auto-

configuration process on a physical link.

Which of the following addresses can be assigned to the interfaces?

A. FEC0:0:0:1::1/64
B. FE80::260:3EFF:FE11:6770/10
C. 2001:0410:0:1:0:0:0:1/64
D. 2002:500E:2301:1:20D:BDFF:FE99:F559/64

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The FE80::260:3EFF:FE11:6770/10 address can be assigned to an interface of the IPv6-enabled router. This address is a link-local address as it has the prefix FE80::/10. Link-local addresses can be configured for an interface either automatically or manually.

Link-local addresses are IPv6 unicast addresses that are configured on the interfaces of an IPv6-enabled router. With link-local addresses, the nodes can connect to a network (local link) and communicate with other nodes. In addition, these addresses participate in the neighbor discovery protocol and the stateless auto-configuration process.

The FEC0:0:0:1::1/64 address should not be used for the interfaces because this address is a site-local address. Site-local addresses are IPv6 equivalent addresses to IPv4's private address classes. These addresses are available only within a site or an intranet, which typically is made of several network links.

You should not use the 2001:0410:0:1:0:0:0:1/64 and 2002:500E:2301:1:20D:BDFF:FE99:F559 addresses for the interfaces. These two addresses are global unicast addresses as they fall in the range from 2000::/3 and to E000::/3. A global address is used on links that connect organizations to the Internet service providers (ISPs).

Objective:
Network Fundamentals

Sub-Objective:
Configure and verify IPv6 Stateless Address Auto Configuration

References:

https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-lla.html

QUESTION 52
RouterA and RouterB, which connect two locations, are unable to communicate. You run the show running-configuration command on both router interfaces, RouterA and RouterB. The following is a partial output:

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

routerB#show running-config
interface Serial1
description Router_B
ip address 192.10.192.1 255.255.255.0
```

encapsulation ppp
no ip mroute-cache
clockrate 64000

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

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

Objective:
Network Fundamentals

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

References:

http://docwiki.cisco.com/wiki/Point-to-Point_Protocol

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

QUESTION 53
Which type of IP address is a registered IP address assigned by the Internet Service Provider (ISP), and represents one or more inside local IP addresses externally?

A. Inside local address
B. Outside local address
C. Inside global address
D. Outside global address

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

An inside global address is a registered IP address assigned by the ISP that represents internal local IP addresses externally.

An inside local address is an IP address (usually private) assigned to a host on the internal network. The inside local address is usually not assigned by the service provider, nor used to represent one or more inside local IP addresses externally

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

An outside global address is the IP address assigned to a host on the external network by the host owner. The address is allocated from a globally routable address space. It is not used to represent one or more inside local IP addresses externally

Objective:
Infrastructure Services

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

References:

https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/4606-8.html

http://www.ciscopress.com/articles/article.asp?p=25273

QUESTION 54
You are the network administrator for your company. You wanted to connect the host computers to the switches.

Which cable should you use to ensure the connectivity?

A. Straight-through cable
B. Rollover cable
C. Crossover cable
D. Serial cable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A straight-through cable is a normal four-pair cable with the same order of pin configuration on both ends. These are usually used to connect a computer to the switch or hub's Ethernet ports. The following table shows

the pin layout of a straight-through cable:

Pin No.	Pin No.
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

A rollover cable, also known as rolled cable or Cisco console cable, is used to connect a computer terminal to the console port of a router. The cable pin order at one end of the cable is the reverse of the order at another end. Pin 1 is connected to pin 8, pin 2 top in 7, and so on.

A crossover cable is used to connect two similar devices such as a computer to computer or a switch to a switch, and a computer to a router's Ethernet port.

A serial cable is used on a router's wide area network (WAN) interface to connect to the serial ports. Cisco serial cables generally have a male DB-25 connector on one end and a female DB-25 connector on the other.

Objective:
LAN Switching Fundamentals

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

References:

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

QUESTION 55
Which feature is NOT provided by flow control?

A. buffering
B. windowing
C. full duplex transmission
D. source-quench messaging

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The full duplex mode of transmission is not provided by flow control. Full duplex transmission is an Ethernet concept where hosts are able to send and receive at the same time. There are no collisions in a full-duplexEthernet network. A dedicated switch port is required for each node in a full-duplex Ethernet network. Both the host's NIC and the switch port must be capable of operating in full-duplex mode. When full duplex is implemented, no collisions will occur on the link between the switch and the device. That will be one error condition that can be removed from consideration when troubleshooting a full duplex link.

Flow control is a function that prevents network congestion. It does so by ensuring that the transmitting device does not flood the receiving device with data. The following statements are true regarding flow control:

- Controls the amount of data which the sender can send to the receiver.
- Uses buffering, transmitting source-quench messages, and windowing to handle network congestion.
- Determines the rate at which the data is transmitted between the sender and receiver.
- Types of flow control include windowing, buffering, and congestion avoidance.

Flow control generally operates at the Transport layer in the OSI model. The Transport layer is responsible for error-free and sequential delivery of data. This layer is used to manage data transmission between devices.

Buffering is a method by which network devices use to save temporary overflows of excess data into the memory. The data is stored in the memory until it is processed.

Source-quench messages are used by the devices that receive the data to avoid buffer overflow.

Windowing is a scheme in which an acknowledgment is required by the source device from the destination after the transmission of a fixed number of packets.

Objective:
Network Fundamentals

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

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

QUESTION 56
Which Cisco Internetwork Operating System (IOS) command is used to apply an access list to an interface?

A. router(config)# ip access-group
B. router(config-if)# ip access-group
C. router(config)# ip access-list
D. router(config-if)# ip access-list

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The router(config-if)#ip access-group command is used to apply an access list to an interface. This command is issued in interface configuration mode. The syntax of the command is as follows:

router(config-if)# ip access-group {access-list-number|access-list-name} {out|in}

The parameters of the command are as follows:

- out|in: Specifies where the access list will be applied on the router. The out value will cause the router to apply the access list to all outgoing packets. The in value will cause the router to apply the access list to all incoming packets.
- access-list-number: Specifies the number of an access list.
- access-list-name: Specifies the name of the access list.

The router(config)# ip access-group command is incorrect because the ip access-group command should be issued in interface configuration mode.

The router(config)# ip access-list command is incorrect because this command is used to define an access list by name.

The router(config-if)# ip access-list command is incorrect because the ip access-groupcommand is issued in global configuration mode, and is used to define an access list by name.

Objective:
Infrastructure Services

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

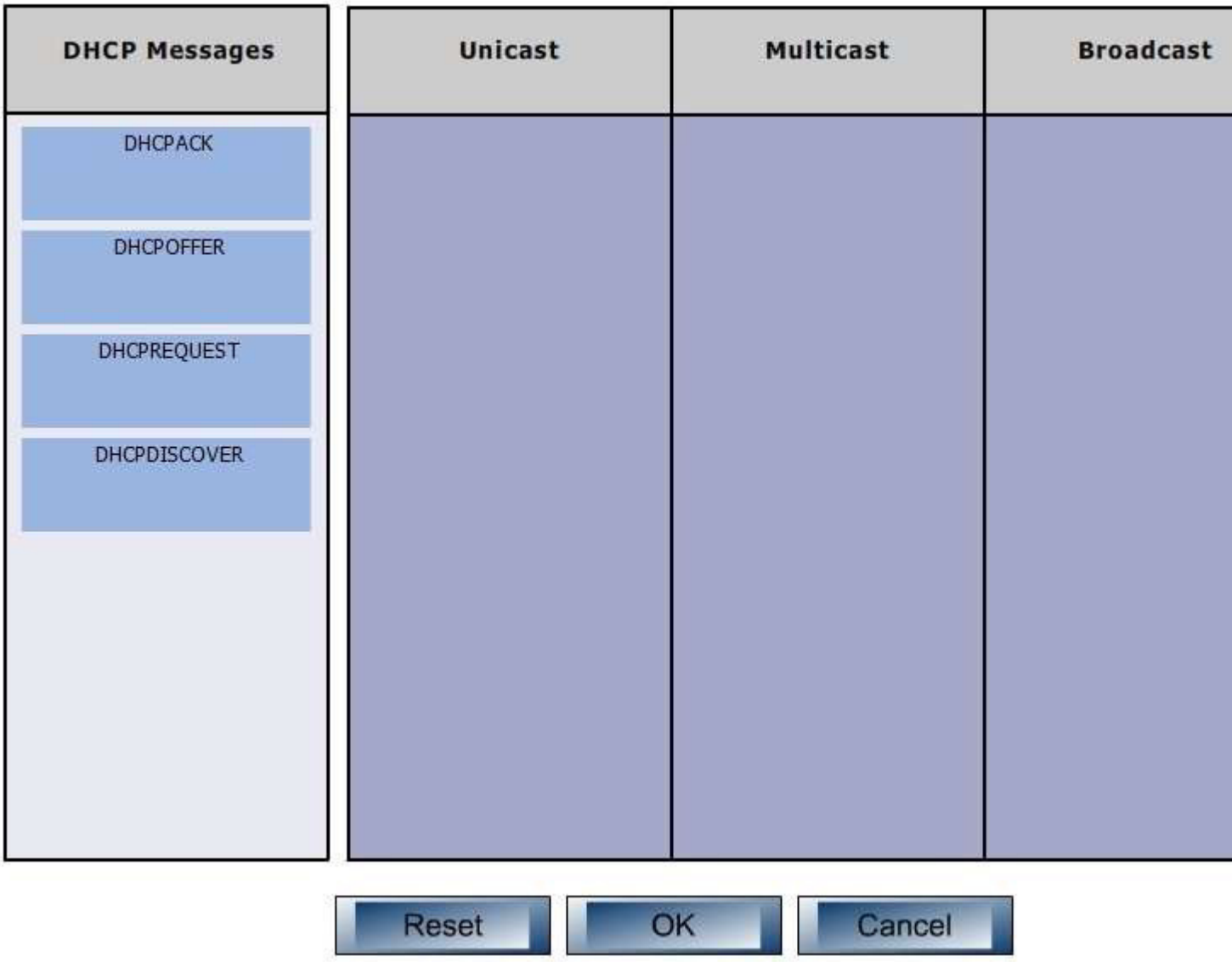
References:

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

QUESTION 57
DRAG DROP
Group the special DHCP messages exchanged over the network, on the left, into the different transmission types, on the right.

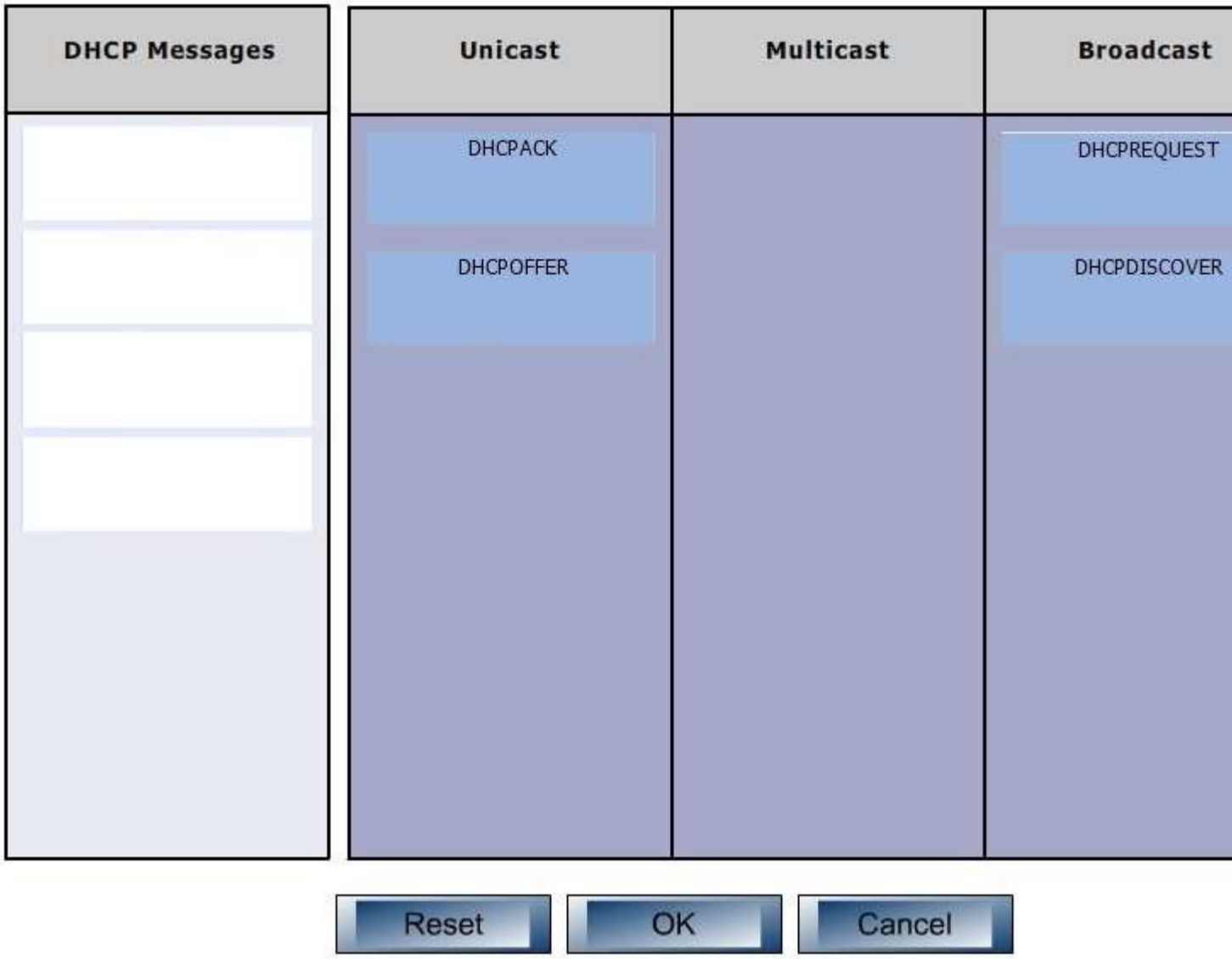
Select and Place:

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



Correct Answer:

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



Section: (none)
Explanation

Explanation/Reference:
Explanation:

Dynamic Host Configuration Protocol (DHCP) is an enhancement over Bootstrap Protocol (BOOTP). DHCP is used to automate the distribution of IP address to clients from a central server. BOOTP protocol was also used distribute IP addresses, but was inflexible when changes were made in the network. DHCP offers the following three advantages, which also addressed the inflexibility of the BOOTP protocol:

- Automatic allocation of permanent IP addresses
- Automatic allocation of time bound (leased) IP addresses
- Provision of assigning static IP address or defining a pool of reserved IP address

The following steps are used to allocate IP address dynamically using a CiscoIOS DHCP server:

1. The client device broadcasts a DHCPDISCOVER broadcast message to locate a Cisco IOS DHCP server.
2. The Cisco IOS DHCP server replies with a DHCPOFFER unicast message containing configuration parameters such as an IP address, a MAC address, a domain name, and a lease for the IP address for the client device.
3. The client sends back a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the Cisco IOS DHCP server.
4. The Cisco IOS DHCP server replies to client device with DHCPACK unicast message acknowledging the allocation of the IP address to this client device.

While DHCP is very useful in reducing the administrative burden of issuing IP configurations in a large network, Cisco best practices call for using static IP addressing in a small (6 or fewer hosts) network.

Objective:
Infrastructure Services

Sub-Objective:
Configure and verify DHCP on a router (excluding static reservations)

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfdhcp.html

QUESTION 58
In which of the following IPv6 address assignment methods will the interface receive its IPv6 address from a process native to IPv6, and receive additional parameters from DHCP?

A. Stateless DHCPv6
B. Stateful DHCPv6
C. DHCPv6-PD
D. Stateless autoconfiguration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Stateless DHCPv6 uses a combination of processes to assign a configuration to an IPv6 interface. It uses Stateless AddressAutoconfiguration (SAAC), a process native to IPv6, to assign an IPv6 address to the interface. It uses DHCPv6 to assign other parameters, such as the DNS server and NTP server.

In stateful DHCPv6, the interface will receive the IPv6 address and all other parameters from the DHCP server.

In DHCPv6 Prefix Designation (DHCPv6-PD), the device is assigned a set of IPv6 "subnets." This assignment will consist of a set of IPv6 addresses in the same subnet (such as the address 2001:db8::/60) that the device can dynamically allocate to its interfaces.

Objective:
Network Fundamentals

Sub-Objective:
Configure and verify IPv6 Stateless Address Auto Configuration

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book/ip6-dhcp-stateless-xe.html

QUESTION 59
Which Cisco IOS command can be used to troubleshoot switch startup problems on a Cisco Catalyst 2950 switch?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

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

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

Objective:
Infrastructure Maintenance

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

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

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

QUESTION 60
Which of the following values will be used by a router to make a routing decision when two routes have been learned from OSPF?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

Objective:
Routing Fundamentals

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

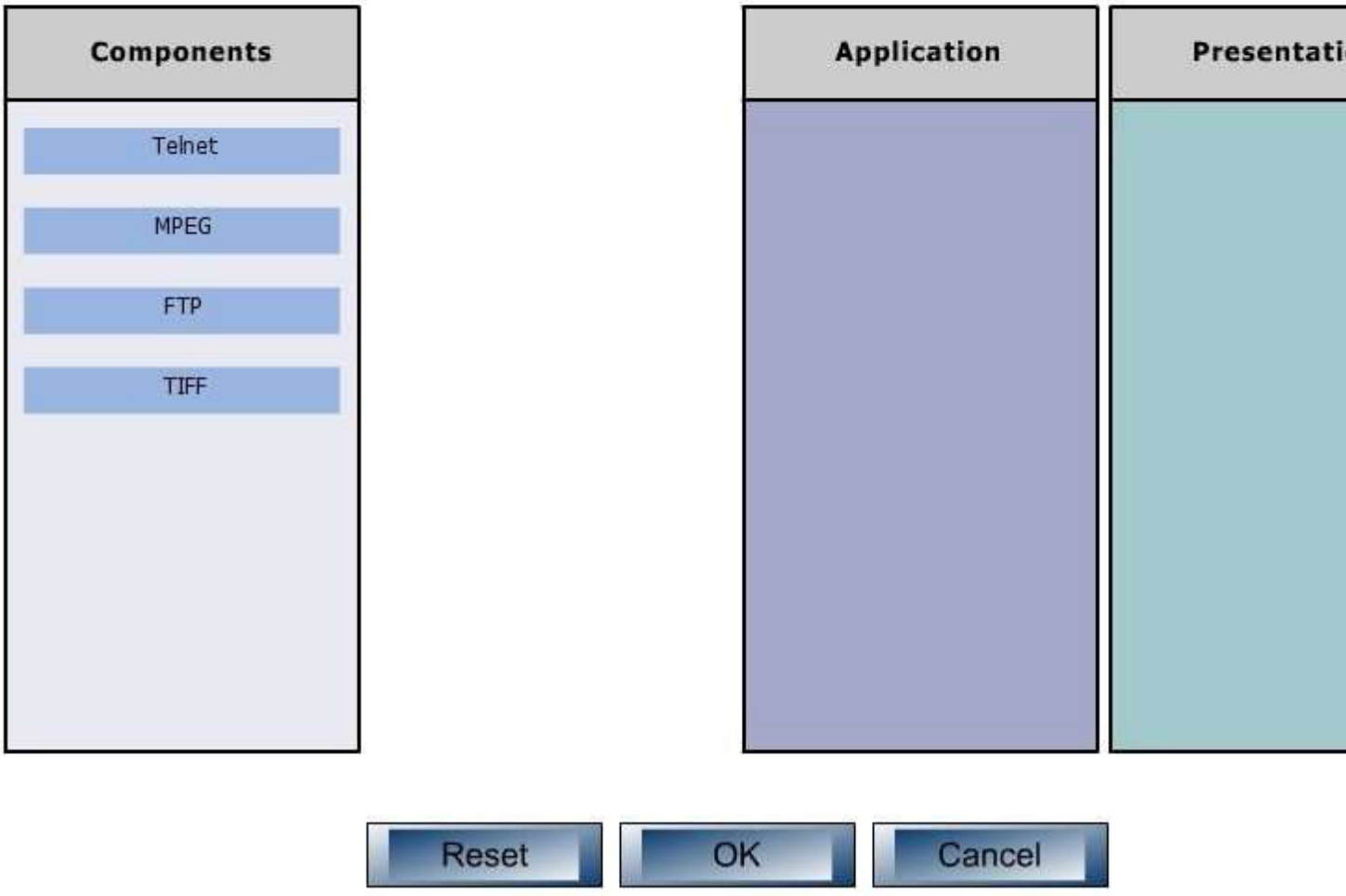
References:

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

QUESTION 61
DRAG DROP
Click and drag the components on the left to their corresponding layers of the Open Systems Interconnection (OSI) model on the right.

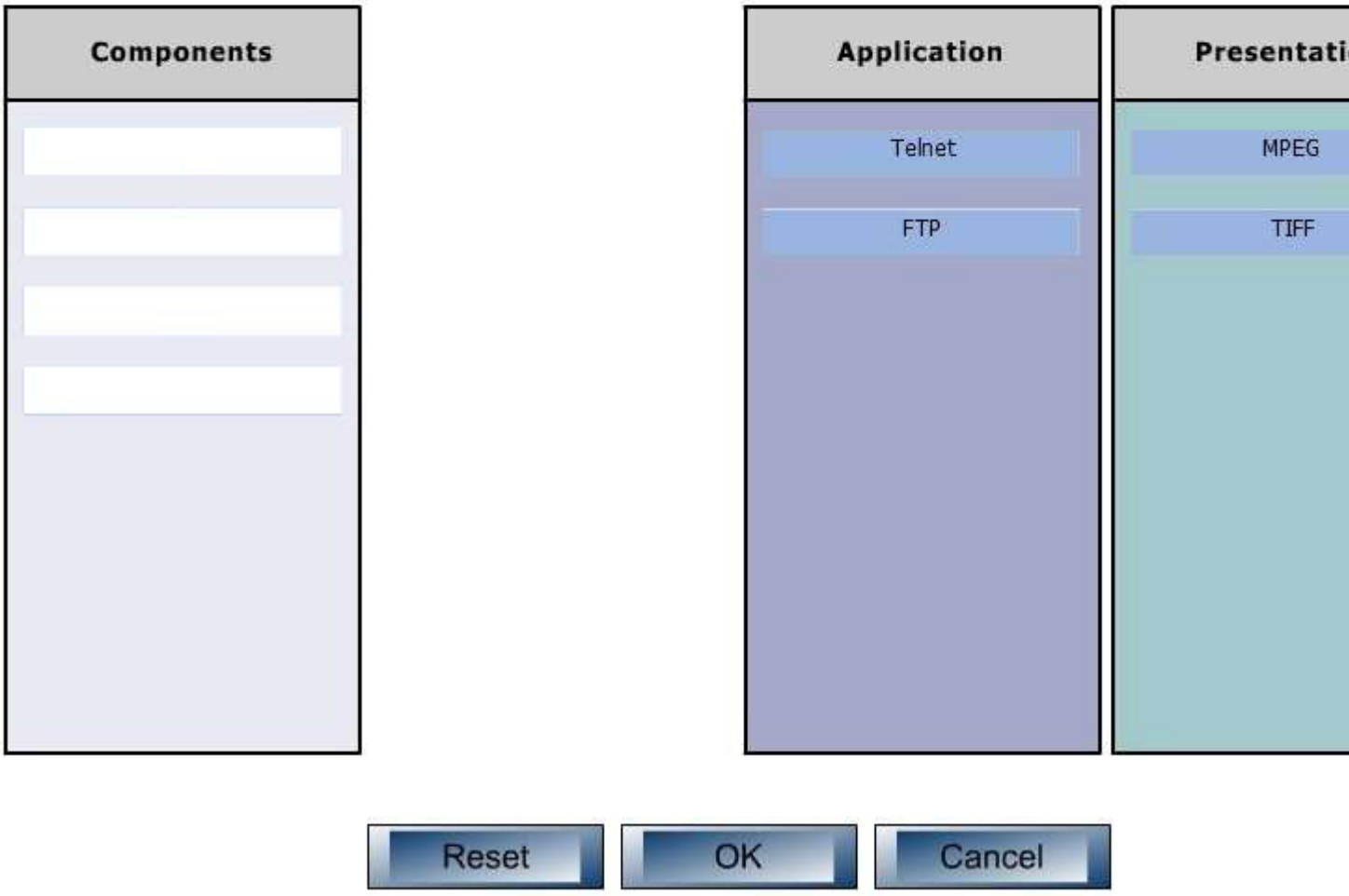
Select and Place:

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



Correct Answer:

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



Section: (none)
Explanation

Explanation/Reference:
Explanation:

File Transfer Protocol (FTP) and Telnet are services, which are implemented at the Application layer in the Open Systems Interconnection (OSI) model. The Application layer is responsible for interacting directly with the application. It provides application services, such as e-mail.

Motion Picture Experts Group (MPEG) and TaggedImage File Format (TIFF) are graphic image formats, which are implemented at the Presentation layer. The Presentation layer enables coding and conversion functions for application layer data. Data is formatted and encrypted at this layer. The Presentation layer converts data into a format which is acceptable to the Application layer.

The following are also OSI layers and their descriptions:

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

Objective:
Network Fundamentals

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

References:

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

QUESTION 62
Examine the following partial output of the show interfaces command.

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

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

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

BW 10000 Kbit

Objective:
LAN Switching Fundamentals

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

References:

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

QUESTION 63
What command was used to generate the output shown below?

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

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

DNS Servers . . . . . : 10.88.10.48
10.75.139.18
NetBIOS over Tcpip. . . . . : Enabled

A. winipcfg
B. ipconfig
C. ifconfig
D. ipconfig/all

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The output displayed is that generated by the ipconfig/all command as executed on a Windows computer. This

command displays a wealth of information about the current configuration. Examples of information that can be gleaned from the sample output include:

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

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

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

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

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

Objective:
Network Fundamentals

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

References:

https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

QUESTION 64
The conference room has a switch port available for use by the presenter during classes. You would liketo prevent that port from hosting a hub or switch. Which of the following commands could be used to prevent that port from hosting a hub or switch?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The switchport port-security command would prevent the port from hosting a hub or switch. This command enables port security on an interface. It does not specify a maximum number of MAC addresses, but in the default is 1, therefore it would accomplish the goal.

The switchport port-security maximum command alone could not be used to limit the number of MAC addresses allowed on the interface to 1. This command has no effect unless the switchport port-security command has been executed.

The switchport port-security mac address sticky command would not prevent that port from hosting a hub or switch. This command is used to allow a port to dynamically learn the first MAC address it sees in the port, add it to the MAC address table and save it to the running configuration of the switch.

The switchport port-security mac address command would not prevent that port from hosting a hub or switch. This command is used to manually assign a MAC address to a port as a secure address. When used in combination with the switchport port-security maximum command, the use of the port can not only be limited to one address at a time, but also limited to only a specific address. For example, the following set of commands would assure that only the device with the MAC address of 0018.cd33.46b3 will be able to connect to the port:

Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 0018.cd33.46b3

Objective:
LAN Switching Fundamentals

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

References:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ewa/configuration/guide/conf/port_sec.html

QUESTION 65
You have successfully configured a router, but it prompts you to run Setup mode every time the router is restarted. Based on the following output, what could be causing this problem?

RouterA# show version

Cisco Internetwork Operating System SoftwareIOS (tm) 2500 Software (C2500-JS-L), Version 11.3(6), RELEASE SOFTWARE (fc1)

Copyright 1986-1998 by Cisco Systems, Inc.
Compiled Tue 06-Oct-98 22:17 by kpma
Image text-base: 0x03048CF4, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)

RouterA uptime is 25 minutes
System restarted by power-on
System image file is "flash:c2500-js-l_113-6.bin", booted via flash

Cisco 2500 (68030) processor (revision D) with 4096K/2048K bytes of memory.
Processor board ID 04203139, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2142

A. The router does not have sufficient flash memory.
B. The configuration register is incorrect.

C. The configuration file could not be found in NVRAM.
D. The router could not locate a configuration file over the network.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The configuration register is incorrect. The configuration register value of 2142 is preventing the router from loading the configuration file from NVRAM.

The router configuration register is used to control various aspects of the router boot sequence, and defaults to a value of 2102. A configuration register of2102 indicates that the router should boot normally, which consists of loading the Internetwork Operating System (IOS) into RAM, then loading the saved configuration file from Non-Volatile RAM (NVRAM) to configure the router.

Changing the configuration register to 2142 tells the router to bypass the saved configuration in NVRAM. This causes the router to boot with a default running configuration, and prompt to run the Initial Configuration Dialog (or Setup mode). Changing the configuration register to 2142is necessary to perform password recovery or to bypass any other aspect of a saved configuration that might be causing problems. After the situation is resolved, the configuration register would then be changed back to the default of 2102 with the following command:

Router(config)# config-register 0x2102

The router is successfully loading the IOS from flash memory, so insufficient flash memory is an incorrect answer.

The configuration register is instructing the router to bypass the configuration file in NVRAM, so it is incorrect to state that the configuration file could not be found in NVRAM.

The configuration register is instructing the router to bypass the configuration file in NVRAM, so it is incorrect to state that the router could not locate a configuration file over the network.

Objective:
Infrastructure Maintenance

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

References:

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

https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_c1.html#wp1068966

QUESTION 66
Which feature enables a host to obtain an IP address from a DHCP server on another subnet?

A. DHCP relay agent
B. DHCP BOOTP agent
C. DHCP relay protocol
D. DHCP BOOTP relay

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

A Dynamic Host Configuration Protocol (DHCP) relay agent enables hosts to obtain IP addresses from a DHCP server on another subnet. Hosts use DHCPDISCOVER broadcast messages to locate the DHCP server because they don't know the location of the DHCP server. Because routers are designed to filter broadcasts, the DHCPDISCOVER packet would be dropped unless the router is configured to forward such packets. Enabling a DHCP relay agent on a Cisco router allows it to receive certain types of broadcasts and forward them to special helper addresses.

The following sequence describes an IP address relay process:

- The DHCP client broadcasts a DHCP request on the network.
- The DHCP request is intercepted by the DHCP relay agent, which inserts the relay agent information option (option 82) in the packet.
- The DHCP relay agent forwards the DHCP packet to the DHCP server.
-The DHCP server uses the suboptions of option 82 in the packet, assigns IP addresses and other configuration parameters, and forwards the packet to the client.
- The relay agent again intercepts the packet and strips off the option 82 information before sending it to the client.

The ip helper-address interface configuration command enables a DHCP relay agent on a Cisco router.

DHCP is an enhancement over Bootstrap Protocol (BOOTP) and is used to automate the distribution of IP address to clients from a central server. The BOOTP protocol was also used distribute IP addresses, but was inflexible to changes in the network. DHCP offers three advantages that also address the inflexibility of the BOOTP protocol:

- Automatic allocation of permanent IP addresses
- Automatic allocation of time bound (leased) IP addresses
- Ability to assign static IP address or define a pool of reserved IP address

When a DHCP relay is unnecessary, the following steps describe the address allocation process:

- The client device broadcasts a DHCPDISCOVER broadcast message to locate a DHCP server.
- The DHCP server replies with a DHCPOFFER unicast message containing configuration parameters, such as an IP address, a MAC address, a domain name, and a lease for the IP address for theclient device.
- The client sends back a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the DHCP server.
- The DHCP server replies back to client device with DHCPACK unicast message, acknowledging the allocation of the IP address to this client device.

While DHCP is very useful in reducing the administrative burden of issuing IP configurations in a large network, Cisco best practices call for using static IP addressing in a small (6 or fewer hosts) network.

All other options are invalid devices or features.

Objective:
Infrastructure Services

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

References:

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

https://www.cisco.com/c/en/us/td/docs/ios/ipapp/command/reference/iap_i1.html#wp1032599

QUESTION 67
What is the possible IP range that can be assigned to hosts on a subnet that includes the address 192.168.144.34/29?

A. 192.168.144.32 - 192.168.144.63
B. 192.168.144.33 - 192.168.144.38
C. 192.168.144.33 - 192.168.144.48
D. 192.168.144.28 - 192.168.144.40

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Range 192.168.144.33 - 192.168.144.38 is the correct answer. To determine the range of addresses that can be assigned in a subnet, you must first determine the network ID of the subnetwork and the broadcast address of the subnetwork. All addresses that can be assigned to hosts will lie between these endpoints. The network ID can be obtained by determining the interval between subnet IDs. With a 29-bit mask, the decimal equivalent of the mask will be 255.255.255.248. The interval between subnets can be derived by subtracting the value of the last octet of the mask from 256. In this case, that operation would be 256 - 248 = 8. Therefore, the interval is 8.

The first network ID will always be the classful network you started with (in this case 192.168.144.0). Each subnetwork ID will fall at 8-bit intervals as follows:

192.168.114.0
192.168.144.8
192.168.144.16
192.168.144.24
192.168.144.32
192.168.144.40

We can stop at the 192.168.144.40 address because the address given in the scenario, 192.168.144.34, is in the network with a subnet ID of 192.168.144.32. Therefore, since the broadcast address for this network will be 1 less than the next subnet ID (192.168.144.39), the valid range of IP addresses is 192.168.144.33 - 192.168.144.38. 192.168.144.39 will be the broadcast address for the next subnet, and 192.168.144.40 will be the first valid address in the next subnet.

None of the other answers is the correct range.

Objective:
Network Fundamentals

Sub-Objective:
Apply troubleshooting methodologies to resolve problems

References:

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

QUESTION 68
Which Cisco Internetwork Operating System (IOS) command is used to copy the configuration stored in Random Access Memory (RAM) to Non-Volatile Random Access Memory (NVRAM)?

A. router# copy running-config startup-config
B. router(config)# copy running-config startup-config
C. router# copy startup-config running-config
D. router(config)# copy startup-config running-config

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The router# copy running-config startup-config command is used to copy the configuration stored in Random Access Memory (RAM) to Non-Volatile Random Access Memory (NVRAM). This command is issued inprivileged EXEC mode. The syntax of the command is as follows:

router# copy running-config startup-config

The parts of the command are as follows:

- running-config is the running configuration stored in RAM.
- startup-config is the startup configuration stored in Non-Volatile Random Access Memory (NVRAM).

The router(config)# copy running-config startup-config command is incorrect because the copy run start command (abbreviated) is not issued in global configuration mode. It is executed in privileged EXEC mode.

The router# copy startup-config running-config command is incorrect because this command is used to copy the configuration stored in NVRAM to RAM.

The router(config)# copy startup-config running-config command is incorrect because neither the copy run start nor the copy start run commands are executed in global configuration mode. Moreover, the copy startup-config running-config command is used to copy the configuration stored in NVRAM to RAM.

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

References:

https://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/mgx_8850/software/mgx_r3/rpm/rpm_r1-1/configuration/guide/appc.html#wp1002710

QUESTION 69
Which command would you use to see which interfaces are currently operating as trunks?

A. show interface switchports
B. show trunk interface
C. show interfaces trunk
D. show switchport trunk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show interfaces trunk command displays a list of interfaces currently operating as trunks, and their configuration (such as supported VLANs or frame tagging method). Sample output would resemble the following:

Switch# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gi0/1 desirable 802.1q trunking 1
Gi0/2 desirable 802.1q trunking 1

Port Vlans allowed on trunk
Gi0/1 1-4094
Gi0/2 1-4094
<<output omitted>>

This output indicates that switch ports Gi0/1 and Gi0/2 are both currently operating as trunks (Status), and that 802.1q frame tagging is being used on the trunk links.

The remaining options are incorrect because they are not valid Cisco IOS commands.

Objective:
Infrastructure Maintenance

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

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

QUESTION 70
Two catalyst switches on a LAN are connected to each other with redundant links and have Spanning Tree Protocol (STP) disabled. What problem could occur from this configuration?

A. It may cause broadcast storms.
B. All ports on both switches may change to a forwarding state.
C. It may cause a collision storm.
D. These switches will not forward VTP information.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The configuration in the scenario may cause broadcast storms. When there are redundant links between two switches, it is recommended that you enable Spanning Tree Protocol to avoid switching loops or broadcast storms. Loops occur when there is more than one path between two switches. STP allows only one active path at a time, thus preventing loops. A broadcast storm occurs when the network is plagued with constant broadcasts. When the switches have redundant links, the resulting loops would generate more broadcasts, eventually resulting in a complete blockage of available bandwidth that could bring the complete network down. This situation is referred to as a broadcast storm.

The option stating that all ports on both switches may change to a forwarding state is incorrect. Forwarding is a port state that is available when using STP. When STP is disabled, the switch cannot change the STP states of its ports.

The option stating that the switches will not forward VLAN Trunking Protocol (VTP) information is incorrect. Enabling or disabling STP does not have a direct effect on VTP messages.

The term collision storm is not a valid term.

Objective:
LAN Switching Fundamentals

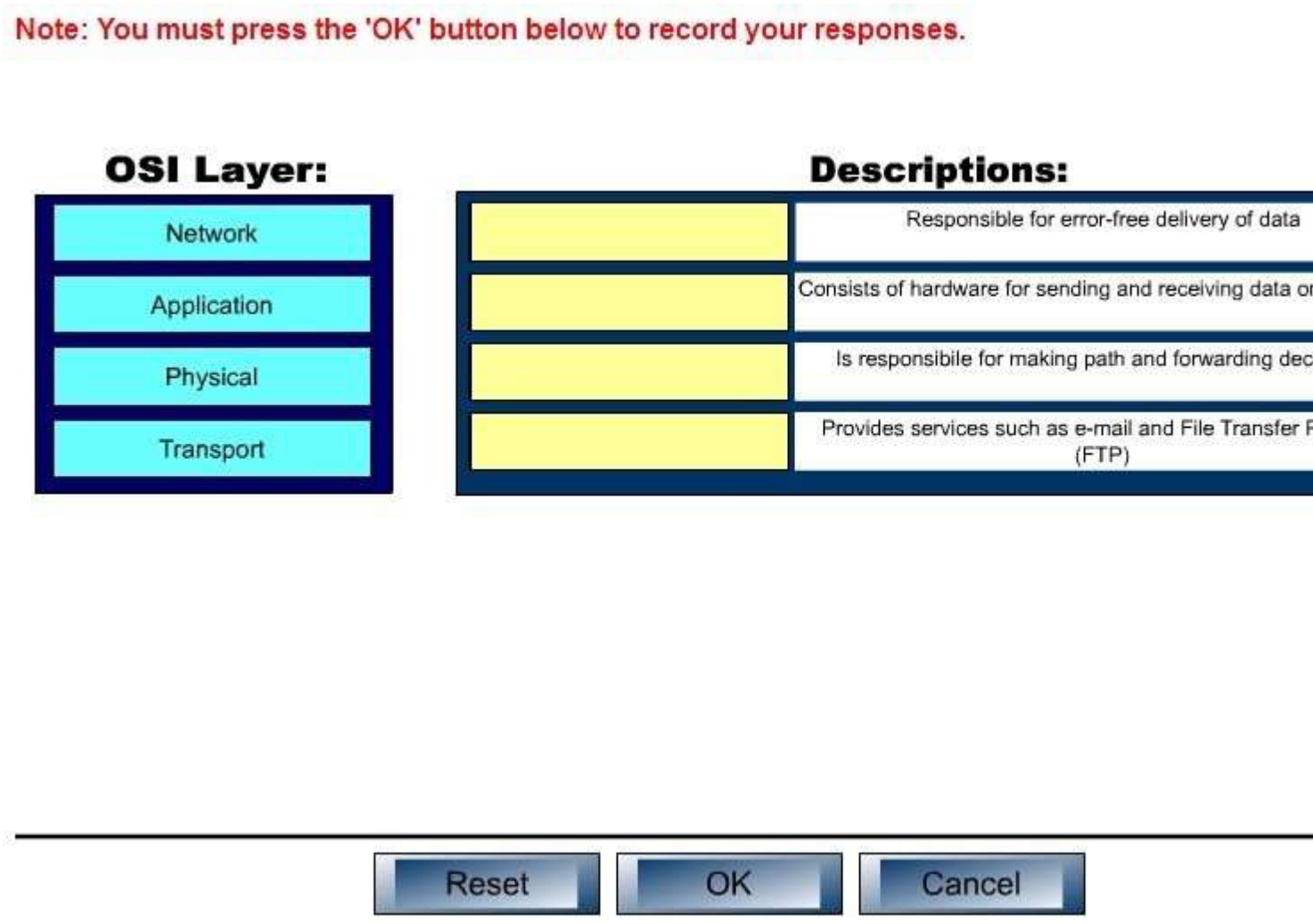
Sub-Objective:
Configure, verify, and troubleshoot interswitch connectivity

References:

https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/12006-chapter22.html#spans

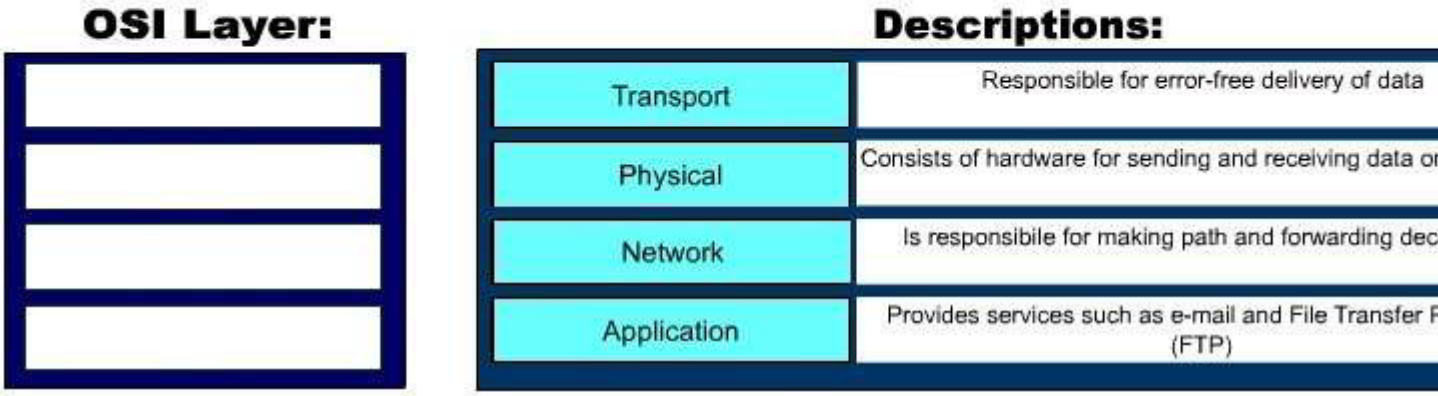
QUESTION 71
DRAG DROP
Click and drag the Open Systems Interconnection (OSI) layers to their corresponding functions on the right.

Select and Place:



Correct Answer:

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



Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following are the OSI layers along with their descriptions:

- Application: Responsible for interacting directly with the application. It provides application services such as e-mail and File Transfer Protocol (FTP).
- Physical: Consists of hardware for sending and receiving data on a carrier. The protocols which work at the Physical layer include Fast Ethernet, RS232, and Asynchronous Transfer Mode (ATM).
- Transport: Responsible for error-free and sequential delivery of data. This layer is used to manage data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Network: Used to define the network address or the Internet Protocol (IP) address, which is then used by the routers to make routing decisions.
- The following are also OSI layers:
- Presentation: Enables coding and conversion functions for application layer data. The formatting and encryption of data is done at this layer. The Presentation layer converts data into a format which is acceptable by the application layer.

- Session: Used to create, manage, and terminate sessions between communicating nodes. The session layer handles the service requests and service responses, which take place between different applications.
- Data Link: Ensures the reliable transmission of data across a network on the basis of Layer 2 addresses such as MAC addresses (Ethernet) or DLCIs (Frame Relay).

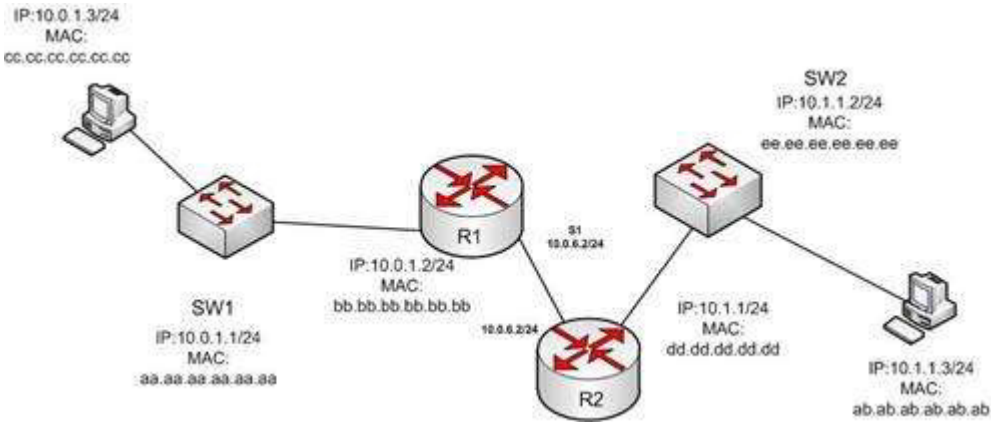
Objective:
Network Fundamentals

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

References:

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

QUESTION 72
In the diagram below, if the workstation at 10.0.1.3 sends a packet to the workstation at 10.1.1.3, what will be the source physical address when the packet arrives at 10.1.1.3?



A. ab.ab.ab.ab.ab.ab
B. ee.ee.ee.ee.ee.ee
C. dd.dd.dd.dd.dd.dd
D. cc.cc.cc.cc.cc.cc
E. aa.aa.aa.aa.aa.aa
F. bb.bb.bb.bb.bb.bb

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The source physical address of the packet when it arrivesat 10.1.1.3 will be that of the interface on the R2 router, dd.dd.dd.dd.dd.dd . Each router will change the MAC address field to the MAC address of its sending interface as it sends the packet and will leave the IP address field unchanged. The switches will change neither field, but will simply use the MAC address field to determine the forwarding path and switch the frame to the port where the MAC address is located. The R2 router is the last device that will make a change to the MAC address field.

The source (10.0.1.3) and destination (10.1.1.3) IP address fields will stay the same at each device. The MAC address field changes when R1 sends the frame to R2 and when R2 send the frame to the workstation at

10.1.1.3.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

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

QUESTION 73
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$7sOd0mgRuXYhHwfWsV4Q2/
!
banner login ^C Welcome to Router 5 Authorized users only ^C
!
interface Ethernet0
ip address 10.1.1.1 255.0.0.0
!
interface Serial0
ip address 20.2.2.2 255.0.0.0
!
router rip
network 10.0.0.0
network 20.0.0.0
!
ip route 0.0.0.0 0.0.0.0 20.2.2.3
!
line vty 0 4
password Cisc0$el1$
no login
!
end
```

What problems exist? (Choose all that apply.)

A. unencrypted privileged mode password
B. inappropriate wording in the banner message
C. weak password on the VTY line
D. Telnet users will not be prompted for a password

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The banner logon message should not contain verbiage that includes the word Welcome. This could potentially supply grounds by a hacker that he was "invited" to access the device.

Also, although a strong password has been configured on the VTY lines, the presence of the no login command instructs the router to NOT prompt for a password.

The login command should be executed under the VTY configuration so that the router will prompt for the password.

The privileged mode password is encrypted because it is listed as an enable secret password.

The password configured on the VTY lines, Cisc0ell, is strong in that it contains numbers, letters, and non-numeric characters and it is at least 8 characters in length.

Objective:
Infrastructure Maintenance

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

References:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf004.html#wp1017507

QUESTION 74
Which of the following statements is TRUE about trunk ports?

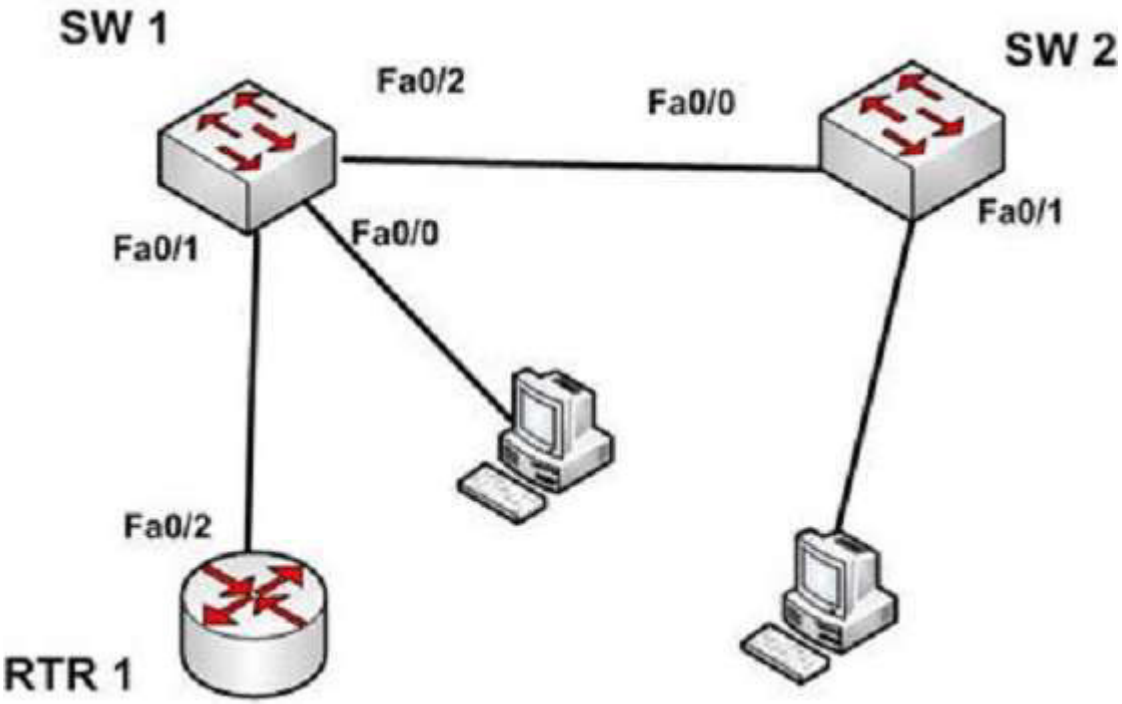
A. A trunk port connects an end-user workstation to a switch.
B. A trunk port uses 802.1q to identify traffic from different VLANs.
C. A trunk port supports a single VLAN.
D. A trunk port uses a straight-through Ethernet cable when connecting two switches.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

A switch port can operate as an access port or a trunk port. An access port is used to connect to an end-user device, such as a workstation, server, or printer,while a trunk port is used to connect to neighboring switches or routers. The trunk link is responsible for carrying data between workstations connected to different switches, or a switch and a router configured for inter-VLAN routing. For example, in the diagram below where VLANs are in use on both switches and inter-VLAN routing is configured, the interfaces will operate as follows:

- SW1 - Fa0/1 and Fa0/2 are trunk links, Fa0/0 is an access link
- SW2 - Fa0/0 is trunk link and Fa0/1 is an access link
-RTR - Fa0/2 is a trunk link



With the exception of frames traveling on the native VLAN, data frames crossing a trunk link must be frame tagged over the link to identify the VLAN that sourced the frame. The receiving switch sees the VLAN ID, and uses this information to forward the frame appropriately. 802.1q and ISL are the two possible frame tagging methods between Cisco switches. In summary, some facts about access and trunk ports:

Access ports:

- Carry traffic for a single VLAN
- Connect end user workstations to the switch
- Use a straight-through cable to connect to the device

Trunk ports:

- Facilitate inter-VLAN communication when connected to a Layer 3 device
- Carry traffic from multiple VLANs
- Use 802.1q to identify traffic from different VLANs

When a new trunk link is created on a switch, all VLANs are allowed to use the trunk, by default.

Trunk ports are used between switches and routers, and do not connect to end-user workstations.

Trunk ports support all VLANs known to the switch by default, so that devices in the same VLAN can communicate across multiple switches. Trunk ports are not limited to a single VLAN, as access ports are.

Trunk ports connected between switches using crossover Ethernet cables, not straight-through Ethernet cables. Trunk ports between switches and routers use straight-through cables.

Objective:
LAN Switching Fundamentals

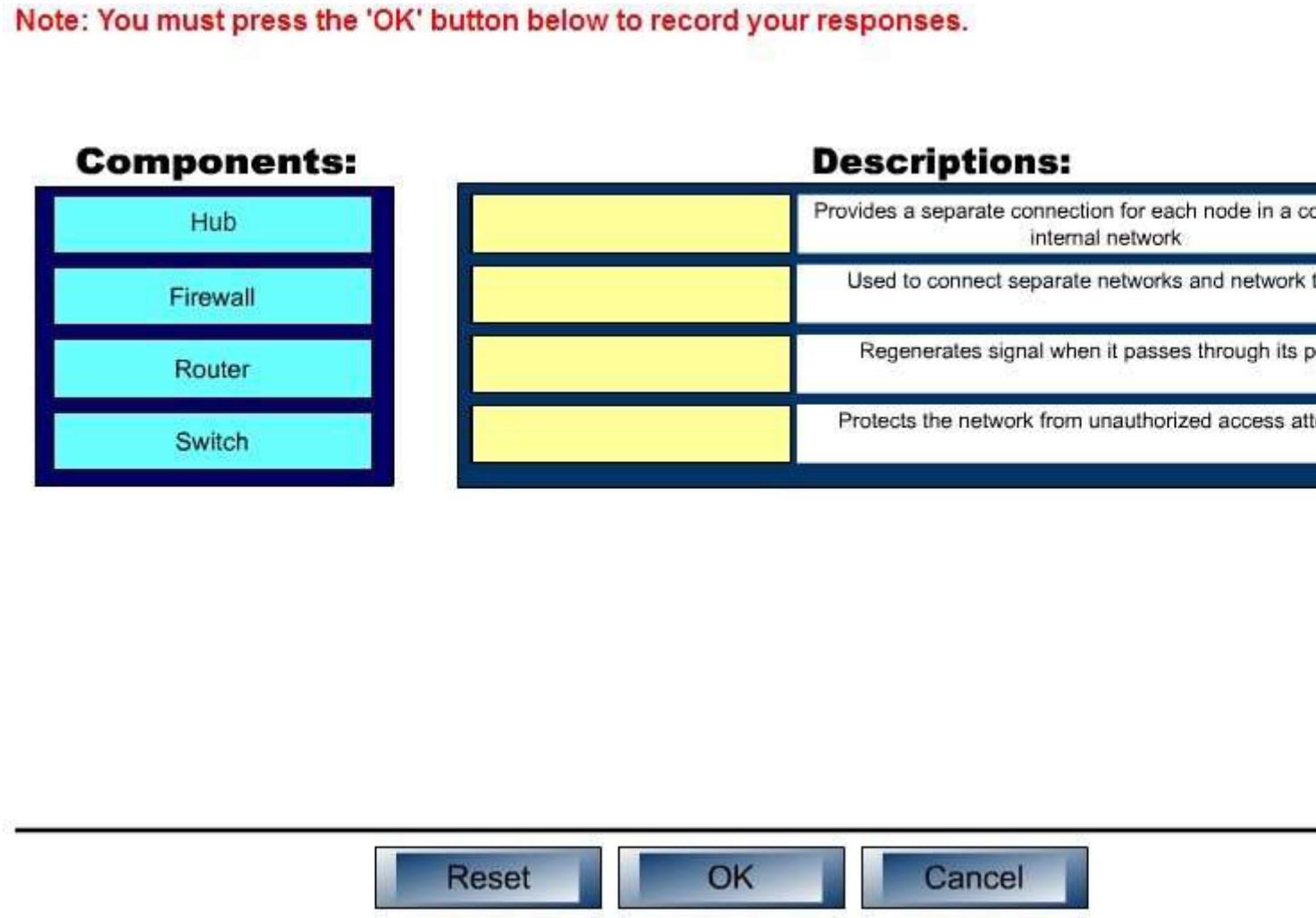
Sub-Objective:
Configure, verify, and troubleshoot interswitch connectivity

References:

http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3

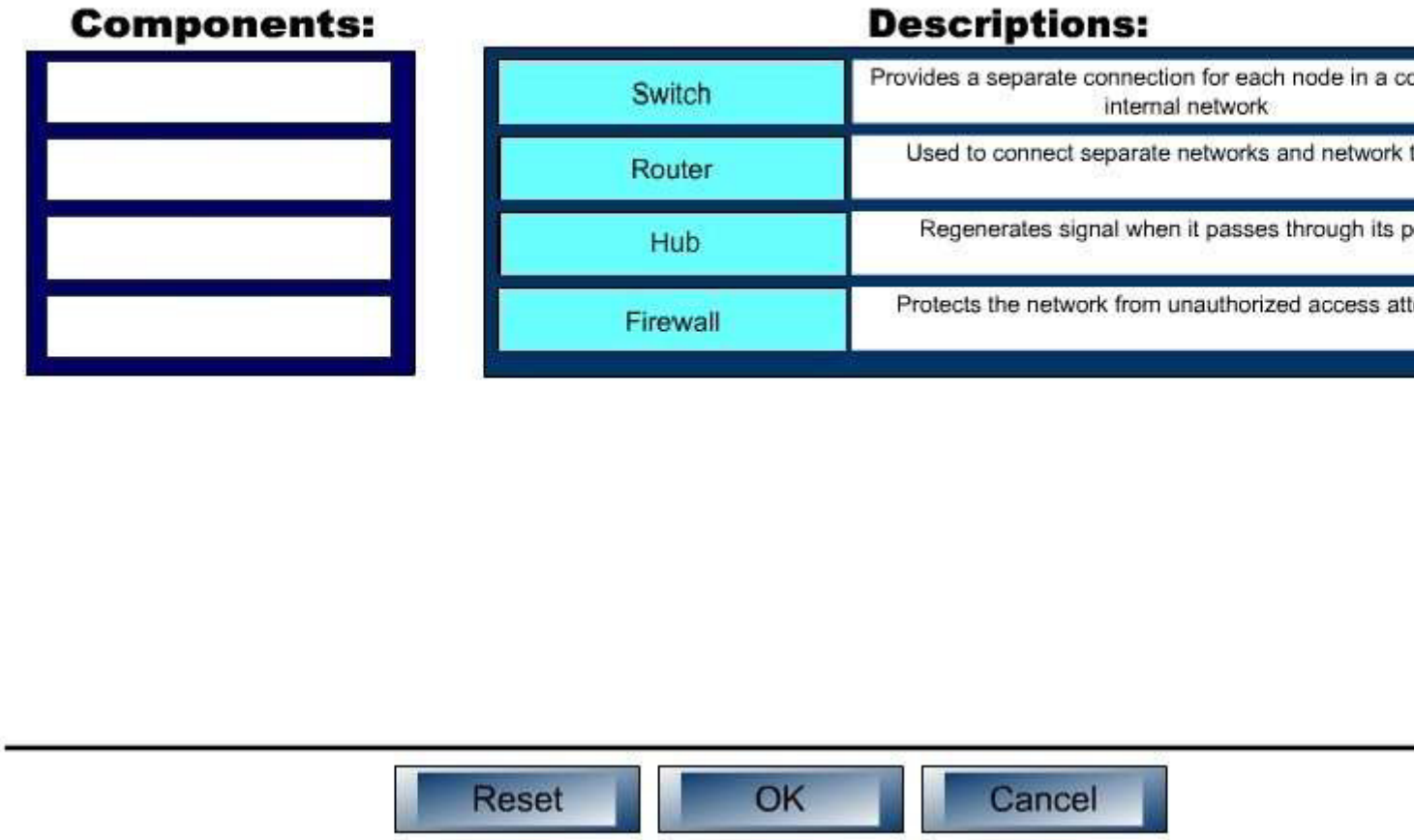
QUESTION 75
DRAG DROP
Click and drag the network devices from the left to their appropriate descriptions on the right.

Select and Place:



Correct Answer:

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

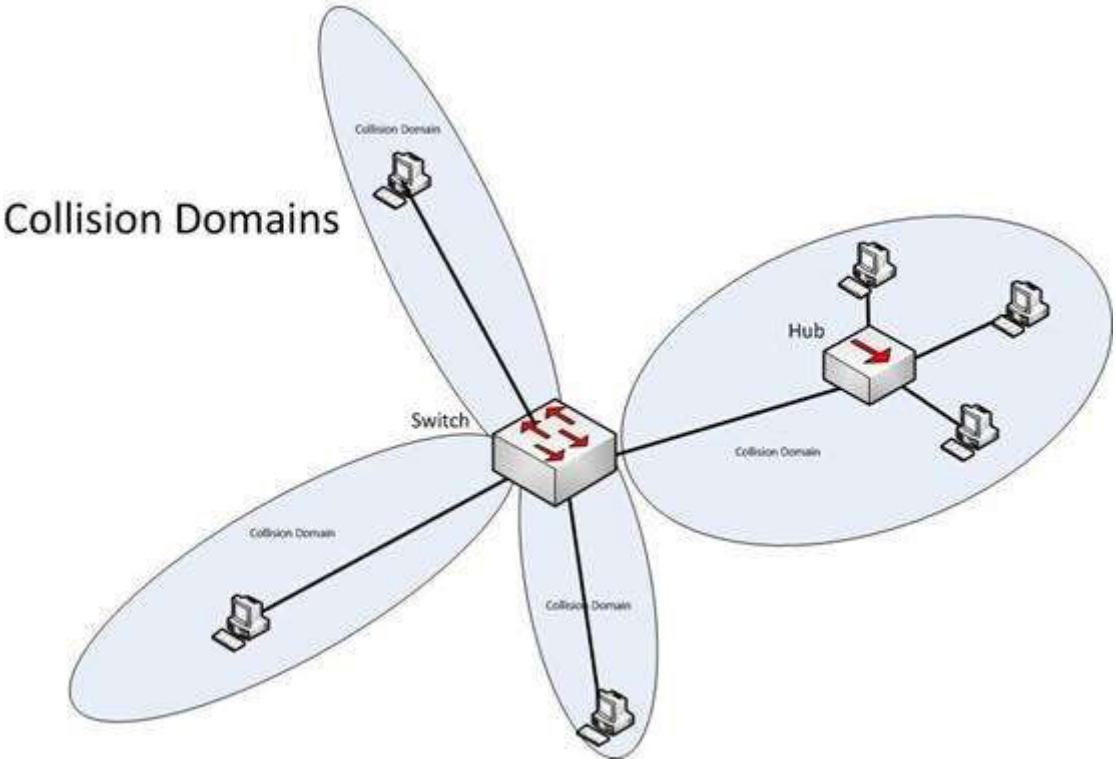


Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following are some of the network devices and their corresponding functions:

- Hub: Regenerates a signal when it passes through its ports. Hubs provide a common connection point for network devices. Hubs are generally used for LAN connectivity and works at Layer 1 of the OSI model.
- Firewall: Protects the network from unauthorized access attempts. It is typically placed between the Internet and aprivate network, but can also be placed between two private networks.
- Router: Provides a means for connecting LAN and WAN segments together. A router separates broadcast domains while connecting different logical and physical networks.
- Switch: Provides a separate collision domain for each node in a company's internal network. Switches work at Layer 2 in the Open System Interconnection (OSI) model and perform their function by observing the source and destination MAC addresses of packets. Because of this method of operation, it can provide dedicated bandwidth to each connected node. Advantages of switches over hubs include the ability to filter frames based on MAC addresses and to allow simultaneous frame transmissions. The diagram below illustrates the ability of a switch to provide a separate collision domain to each device, as compared to the hub, which cannot.



Objective:
Network Fundamentals

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

References:

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

QUESTION 76
Refer to the following partial output of the show interfaces command:

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

What are the two troubleshooting steps that you should perform to resolve the problem depicted in the output? (Choose two.)

A. Check the cable connections.
B. Reset the equipment.
C. Check the router configuration.
D. Check the router configuration for the shutdown interface command.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You should check the cable connections and reset the equipment to troubleshoot the problem depicted in the output. The Serial 0 is down, line protocol is down message indicates that there is no carrier detect (CD) signal sensed by the router. This problem might be due to incorrect cabling or a possible hardware failure.

A complete list of the possible troubleshooting steps that should be performed to resolve this issue include:

- Checking the cable connections.
- Resetting the equipment.
- Checking the CD LED on the CSU/DSU.
- Reporting the issue to the leased-line provider.
- Replacing the faulty equipment.

The router configuration is not a possible issue in this scenario because both serial 0 and line protocol are down, indicating a problem in the physical layer. Configuration issues, such as an incorrect IP address, would be indicated in the second section of the output (line protocol is up/down). The second section, regardless of whether it says up or down is meaningless when the first section indicates a problem.

You should not check the router configuration for the shutdown interface command. When an interface has been manually shut down with this command, it will be indicated in the output as Serial 0 is administratively down, line protocol is down.

Objective:
LAN Switching Fundamentals

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

References:

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

https://www.cisco.com/c/en/us/products/collateral/routers/1700-series-modular-access-routers/prod_end-of-life_notice0900aecd8044473f.html

QUESTION 77
You know that Router2 is configured for RIP. Which Cisco Internetwork Operating System (IOS) command is used to view the current state of all active routing protocols?

A. show ip arp
B. debug ip rip
C. show ip protocols
D. show ip routing process

E. show arp
F. show interfaces

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The show ip protocols command is used to view the current state of active routing protocols. This command is issued from Privileged EXEC mode. The syntax of the command is as follows:

```
Router2# show ip protocols
```

Output of the command would resemble the following:

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 2 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
Ethernet0 2 2 trees
Fddi0 2 2
Routing for Networks:
201.19.0.0
16.2.0.0
10.3.0.0
Routing Information Sources:
Gateway Distance Last Update
201.19.0.9 120 00:00:25
16.2.0.10 120          00:03:10
10.33.0.15 120 00:00:57
Distance: (default is 120)
```

This command shows additional information about individual protocols. The version number of RIP being used is shown on the seventh line of the output. This output also indicates on lines 12-14 that it is routing for three networks: 201.19.0.0, 16.2.0.0, and 10.3.0.0. This means that the router will be sending and receiving RIP updates on any interfaces that have IP addresses in those networks.

Also note that the router at 16.2.0.10 has not sent an update in 3 minutes and 10 seconds. If an update is not received in 50 seconds (for a total of 4 minutes), the route-flush timer (240 seconds from the last valid update) will have expired, causing the local router to remove all networks learned from the router at 16.2.0.10 from the routing table.

For more specific information about those interfaces, in terms such as S0 or Fa0/0, you could execute the show ip interface brief command as shown below. The output displays the addresses of the interfaces, which would indicate which interfaces were enabled for RIP and thus sending and receiving updates.

Router# show ip interface brief
Interface IP-Address OK? Method Status
Fastethernet0/0 201.19.0.8 Yes manual up
Serial0/0 16.2.0.1 Yes manual up

Serial0/1 10.33.0.9 Yes manual up

The show ip arp command is incorrect because this command is executed on a router to determine the IP and MAC addresses of hosts on a LAN connected to the router.

The debug ip rip command is incorrect because this command is used to capture RIP traffic between the routers in real time. This command could also be used to determine the version of RIP being used as shown in line 2 of the partial output of the command below:

Router2#debug ip rip
RIP protocol debugging is on

*Mar 3 02:11:39.207:RIP:received packet with text authentication 234
*Mar 3 02:11:39.211:RIP:received v1 update from 122.108.0.10 on Serial0
*Mar 3 02:11:39.211:RIP: 79.0.0.0/8 via 0.0.0.0 in 2 hops
*Mar 3 02:11:40.212:RIP: ignored v2 packet from 192.168.5.6 (illegal version)

In the above output Router 2 has received a version 1 update from a router at 122.108.0.10 which indicates that a ping to that router should succeed. It also shows what was learned from the router at 122.108.0.10, which is the router to network 79.0.0.0/8 via 0.0.0.0. The 0.0.0.0 indicates that the next hop for that route is the router that sent this advertising (the router at 122.108.0.10).

The output also shows that a RIP router at 192.168.5.6 sent a version 2 update that was ignored by Router 2, which is using version 1. This mismatch of versions will prevent Router 2 from forming an adjacency with the router at 192.168.5.6.

Note: Before running any debug command you should execute the show processes command and verify that the CPU utilization on the router is low enough to handle the effects of running the debug command.

The show ip routing process command is incorrect because it is not a valid Cisco IOS command.

The show arp command is used to identify the IP address to MAC address mappings the router has leaned through the ARP broadcast process. It is helpful when you have identified errors associated with a MAC address and you need to learn the IP address or vice versa. Sample output is below.

router# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.0.0.3 0 0004.dd0c.ffcb ARPA Ethernet01
Internet 10.0.0.1 - 0004.dd0c.ff86 ARPA Ethernet0

The difference between the show arp command and the show ip arp command is that show arp will also include mappings learned throughnon-IP protocols such as when inverse ARP is used to learn and map DLCIs to IP addresses.

The show interface command can also be used to identify IP addresses from MAC addresses and vice versa, but also indicates the state of the interface; IP addresses MTU and much more about each interface. Sample output is below.

router# show interfaces
Ethernet 0 is up, line protocol is up
Hardware is MCI Ethernet,address is 0000.0c00.750c(bia 0000.0c00.750c)
Internet address is 10.108.28.8, subnet mask is255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Objective:
Routing Fundamentals

Sub-Objective:
Interpret the components of routing table

References:

https://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfindp2.html#wp1022264

QUESTION 78
Which two are the limitations of the service password-encryption command? (Choose two.)

A. It uses the MD5 algorithm for password hashing.
B. It uses the Vigenere cipher algorithm.
C. An observer cannot read the password when looking at the administrator's screen.
D. The algorithm used by this command cannot protect the configuration files against detailed analysis by attackers.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following are limitations of the service password-encryption command:

- It uses the Vigenere cipher algorithm, which is simple in nature.
- A cryptographer can easily crack the algorithm in a few hours.
- The algorithm used by this command cannot protect the configuration files against detailed analysis by attackers.

The service password-encryption command does not use the MD5 algorithm for password hashing. The MD5 algorithm is used by the enable secret command.

The option stating that an observer cannot read the password when looking at the administrator's screen is incorrect because this is an advantage of the service password-encryption command.

Objective:
Infrastructure Maintenance

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

References:

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

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

QUESTION 79
A device has an address of 192.168.144.21 and a mask of 255.255.255.240. What will be the broadcast address for the subnet to which this device is attached?

A. 192.168.144.23
B. 192.168.144.28
C. 192.168.144.31
D. 192.168.144.32

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

The broadcast address for the subnet to which this device is attached will be 192.168.144.31.

To determine the broadcast address of a network where a specific address resides, you must first determine the network ID of the subnetwork where the address resides. The network ID can be obtained by determining the interval between subnet IDs. With a 28-bit mask, the decimal equivalent of the mask will be 255.255.255.240. The interval between subnets can be derived by subtracting the value of the last octet of the mask from 256. In this case, that operation would be 256 - 240. Therefore, the interval is 16.

The first network ID will always be the classful network you started with (in this case 192.168.144.0). Then each subnetwork ID in this network will fall at 16-bit intervals as follows:

192.168.144.0
192.168.144.16
192.168.144.32
192.168.144.48

At 192.168.144.48 we can stop, because the address that we are given as a guide is in the network with a subnet ID of 192.168.144.16. Therefore, since the broadcast address for this network will be 1 less than the next subnet ID (192.168.144.32), the broadcast address for the subnet to which this device is attached is 192.168.144.31.

All the other options are incorrect because none of these will be the broadcast address for the subnet to which this device is attached.

Objective:
Network Fundamentals

Sub-Objective:
Applytroubleshooting methodologies to resolve problems

References:

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

QUESTION 80
Which three statements are TRUE regarding static route assignments? (Choose three.)

A. A single static route cannot respond to network outages.
B. Static routes respond to network outages.
C. Static routes are used to discover the network destinations automatically.
D. Static routes are removed from the routing table if the interface goes down.
E. Static routes are not removed from the routing table if the interface goes down.
F. Static routes are manually configured on the router.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following statements are true regarding static route assignments:

- A single static route cannot respond to network outages.
- Static routes are removed from the routing table if the interface goes down.
- Static routes are manually configured on the router.

- Static routes have several advantages over dynamic routing, including the following:
- No routing protocol overhead is generated by the router if static routes are configured.
- No bandwidth is consumed by route advertisements between network devices.
- Router resources are more efficiently used.
- Network security is increased by using static routes.

The option stating that static routes respond to the network outages is incorrect because static routes do not respond to network outages.

The option stating that static routes are used to discover the network destinations automatically is incorrect because dynamic routing protocols are used to discover the network destinations automatically.

The option stating that static routes are not removed from the routing table if the interface goes down is incorrect. Static routes are removed from the routing table if the necessary interface goes down and the destination network is unreachable.

Objective:
Routing Fundamentals

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

References:

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

QUESTION 81
Which command(s) will enable you to configure only serial interface 0 on a Cisco router?

A. router>interface serial 0
B. router#interface serial 0
C. router(config)#interface serial 0
D. router(config-if)#interface serial 0

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

You can use either the router(config)# interface serial 0 command or the router(config-if)# interface serial 0 command to configure serial interface 0 on the router. To perform configuration changes on a single interface, you must either enter interface configuration mode for that interface, or simply execute the command to enter configuration mode for another interface while still at the configuration prompt for the previous interface.

Router configuration mode (as indicated by the prompt router(config)#) allows global configuration of the router. This mode, also referred to as the global configuration mode, must be entered as a precursor to entering the interface configuration mode for a specific interface. The sequence of commands and prompts to arrive at this mode would be:

Router> enable (enters privileged mode)
Router#config t (enters global configuration mode, t is short for terminal)
Router(config)# interface serial 0 (enters interface configuration mode for the serial 0 interface)
Router(config-if)#

At this point, any commands executed would be configuration changes limited to the serial 0 interface. For example, to place an address on the interface, enable the interface, and save the configuration, the command series and prompts would be:

Router> enable
Router# config t
Router(config)# interface serial 0
Router(config-if)# ip address 192.168.20.1 255.255.255.0 (addresses the interface)
Router(config-if)# no shutdown (enables or "turns on" the interface)
Router(config-if)# exit (exits global configuration mode)
Router(config)# exit (exits privileged mode)
Router# copy running-config startup config (copies the changes to the configuration file on the router)

Alternately, you could enter interface configuration mode for one interface while still in configuration mode for another interface, as shown below. After entering the interface serial 1 command, you will be editing serial 1 instead of serial 0.

Router(config)# interface serial 0
Router(config)#
Router(config)# interface serial 1

You should not use the command router> interface serial 0. User EXEC mode, as indicated by the prompt router>, provides limited access to a router and is the initial mode you see after authenticating to the router. The subcommand interface serial 0 is not functional before you proceed to global configuration mode and interface configuration mode for a specific interface.

You should not use the command router# interface serial 0. Privileged mode (as indicated by the prompt router#) must be traversed to get to global configuration mode before you can execute the subcommand interface serial0. This subcommand is not functional while you are still in privileged mode.

Objective:
Infrastructure Maintenance

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

References:

https://search.cisco.com/search?query=Cisco%20IOS%20IP%20Routing%20BFD%20Configuration%20Guide&locale=enUS&tab=Cisco

https://www.cisco.com/c/en/us/obsolete/routers/cisco-1600-series-routers.html

QUESTION 82
A user in your network is having trouble accessing resources and the Internet. You decide to examine the partial output of the ipconfig/all command on his machine. The output is shown below:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\TroyMcClure > ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : KREMLIN0120
   Primary Dns Suffix  . . . . . . . : kappa.alpha.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : kappa.alpha.com

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : triad.rr.com
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-N 7260
   Physical Address. . . . . . . . . : F8-16-54-12-E3-69
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
   DNS Servers . . . . . . . . . . . : 192.168.0.50
```

Which of the following statements describes the user's problem?

A. The default gateway address is incorrect
B. The IP address of the device is incorrect
C. There is no DNS server configured
D. IP routing is not enabled

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The IP address of the device is incorrect. It is not in the same subnet as the default gateway address. While it is possible that the default gateway address is incorrect, that is not as likely a reason, given the fact that the DNS server is also in the same IP subnet as the default gateway.

There is a DNS server configured and its IPaddress is 192.168.0.50. If a DNS server were not configured, this user would be unable to access the Internet, even if all IP addressing problems were resolved.

IP routing is NOT enabled. However, it is not required to be enabled because this device is not acting as a router. The device does not need IP routing enabled to access resources and the Internet if all other IP addressing issues are resolved.

Objective:
Infrastructure Services

Sub-Objective:

Describe DNS lookup operation

References:

http://networking.nitecruzr.net/2005/05/reading-ipconfig-and-diagnosing.html

QUESTION 83
You have a router that is not syncing with its configured time source. Which of the following is NOT a potential reason for this problem?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

Objective:
Infrastructure Services

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

References:

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

QUESTION 84
You are the network administrator for your company. You are in the process of verifying the configuration of the network devices to ensure smooth network connectivity. You want information on the routes taken by packets so that you are able to identify the network points where packets are getting dropped.

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

A. tracert
B. traceroute

C. extended ping
D. ping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

Type escape sequence to abort.
Tracing the route to 33.0.0.4

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

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

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

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

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

Objective:
Routing Fundamentals

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

References:

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

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

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

QUESTION 85
Which of the following is NOT an advantage of static routes over dynamic routing protocols?

A. Routing protocol overhead is not generated by the router.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

The following are disadvantages of static routes:

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

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

Objective:
Routing Fundamentals

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

References:

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

QUESTION 86
You are considering a candidate for a job as a Cisco network technician. As part of the assessment process, you ask the candidate to write down the commands required to configure a serial interface, in the proper order with the correct command prompts. The candidate submits the set of commands shown below (line numbers are for reference only):

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

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

A. The prompt is incorrect on line 1
B. The IP address is missing a subnet mask
C. The prompt is incorrect on line 5
D. The prompt is incorrect on line 3

E. The command on line 4 is incorrect
F. The prompt is incorrect on line 4
G. The description command must be executed before the interface is enabled

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

The correct prompts and commands are as follows:

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

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

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

Objective:
Network Fundamentals

Sub-Objective:
Apply troubleshooting methodologies to resolve problems

References:

https://search.cisco.com/search?query=Cisco%20IOS%20IP%20Routing%20BFD%20Configuration%20Guide&locale=enUS&tab=Cisco

QUESTION 87
When a packet is forwarded through a network from one host to another host, which of the following fields in the Ethernet frame will change at every hop?

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

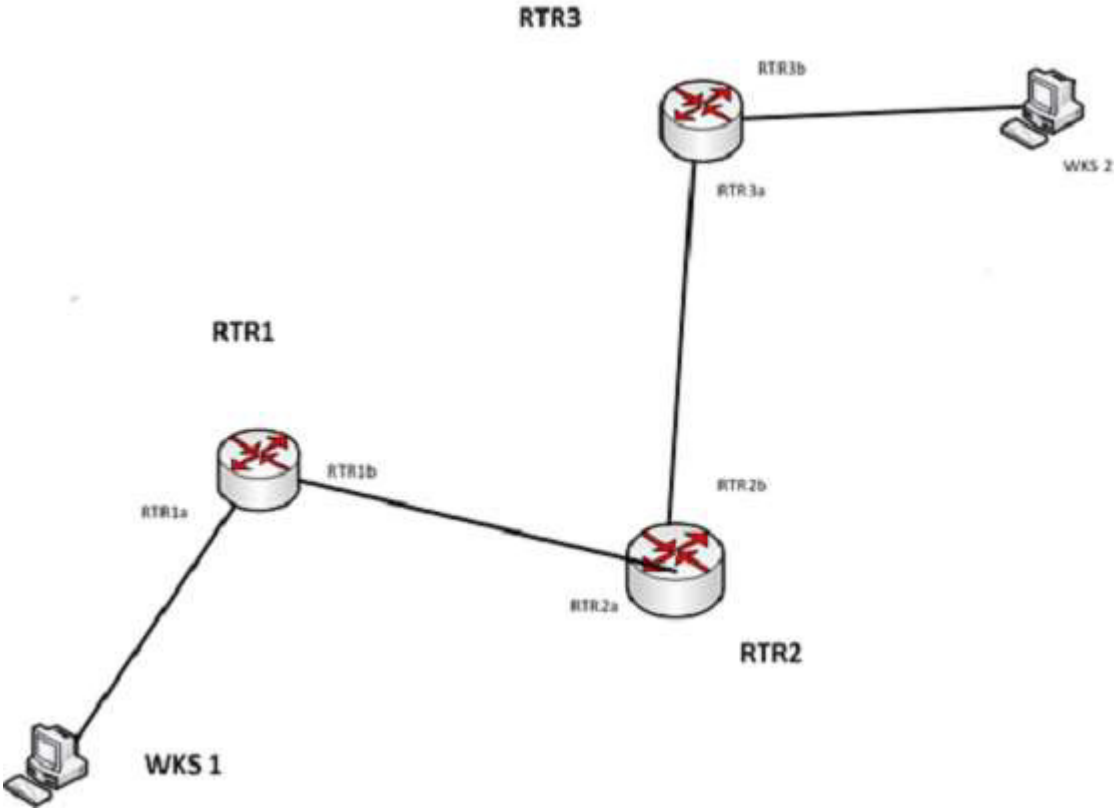
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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



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

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

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

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

As you can see, the destination IP address in the packet does not change, but the MAC address in the frame

changes at each handoff.

Objective:
LAN Switching Fundamentals

Sub-Objective:
Interpret Ethernet frame format

References:

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

QUESTION 88
What configuration is needed to span a user defined Virtual LAN (VLAN) between two or more switches?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

Objective:
LAN Switching Fundamentals

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

References:

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

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

QUESTION 89

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

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

Router(config)# access-list 10 deny any

or

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

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

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

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

or

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

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

access-list 101 permit tcp any any range 1024 65535

Objective:
Infrastructure Services

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

References:

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

QUESTION 90
You are creating a configuration to use on a switch. The configuration must enable you to remotely manage the switch. Which of the following command sets is correct? (Assume the commands are executed at the correct prompt.)

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The following command set is correct:

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

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

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

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

interface fastethernet 0/1
ip address 192.168.20.244 255.255.255.240
no shutdown
exit
ip default-gateway192.168.20.241
line vty 0 15
password cisco
login
exit

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

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

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

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

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

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

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

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

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure and verify device management

References:

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

QUESTION 91

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

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

QUESTION 92
Which show interfaces command output indicates that the link may not be functional due to a Data Link layer issue, while the Physical layer is operational?

A. Ethernet 0/0 is up, line protocol is up
B. Ethernet 0/0 is up, line protocol is down
C. Ethernet 0/0 is down, line protocol is up
D. Ethernet 0/0 is down, line protocol is down

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The first or left-hand column (Ethernet 0/0 is up) indicates the Physical layer state of the interface, while the second or right-hand column (line protocol is down) indicates the Data Link layer state of the interface. The following command output excerpt indicates that the link is not functional due to a Data Link layer (or "line

protocol") issue, while the Physical layer is operational:

Ethernet 0/0 is up, line protocol is down

If the problem were at the Data Link layer while the Physical layer is operational, the show interfaces command output will indicate that the interface is up, but the line protocol is down.

In the normal operation mode, when both Physical layer and Data Link layer are up, the show interfaces output will display the following message:

Ethernet0/0 is up, line protocol is up

The message Ethernet 0/0 is down, line protocol is up is not a valid output.

The message Ethernet 0/0 is down, line protocol is down indicating that both the Physical layer and the Data Link layer are down. Therefore, this is an incorrect option.

Objective:
LAN Switching Fundamentals

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

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

QUESTION 93
Which Cisco IOS command allows you to change the setting of the configuration register?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

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

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

Configuration register is 0x2102
```

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

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

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

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

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

Objective:
Infrastructure Maintenance

Sub-Objective:
Perform device maintenance

References:

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

QUESTION 94
Which of the following situations could cause a switch to enter initial configuration mode upon booting?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

Objective:
Infrastructure Maintenance

Sub-Objective:
Configure and verify initial device configuration

References:

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

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

QUESTION 95
Which two modes are Cisco Internetwork Operating System (IOS) operating modes? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

- User EXEC mode: The commands in this mode are used to enable connections to remote devices and

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

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

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

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

Objective:
Infrastructure Maintenance

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

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

QUESTION 96
Which Ethernet LAN contention or access method listens for a signal on the channel before transmitting data, and stops transmitting if a collision is detected?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

Objective:
LAN Switching Fundamentals

Sub-Objective:
Describe and verify switching concepts

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

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

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

QUESTION 97
Which of the following methods will ensure that only one specific host can connect to port F0/1 on a switch? (Choose two. Each correct answer is a separate solution.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

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

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

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

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

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

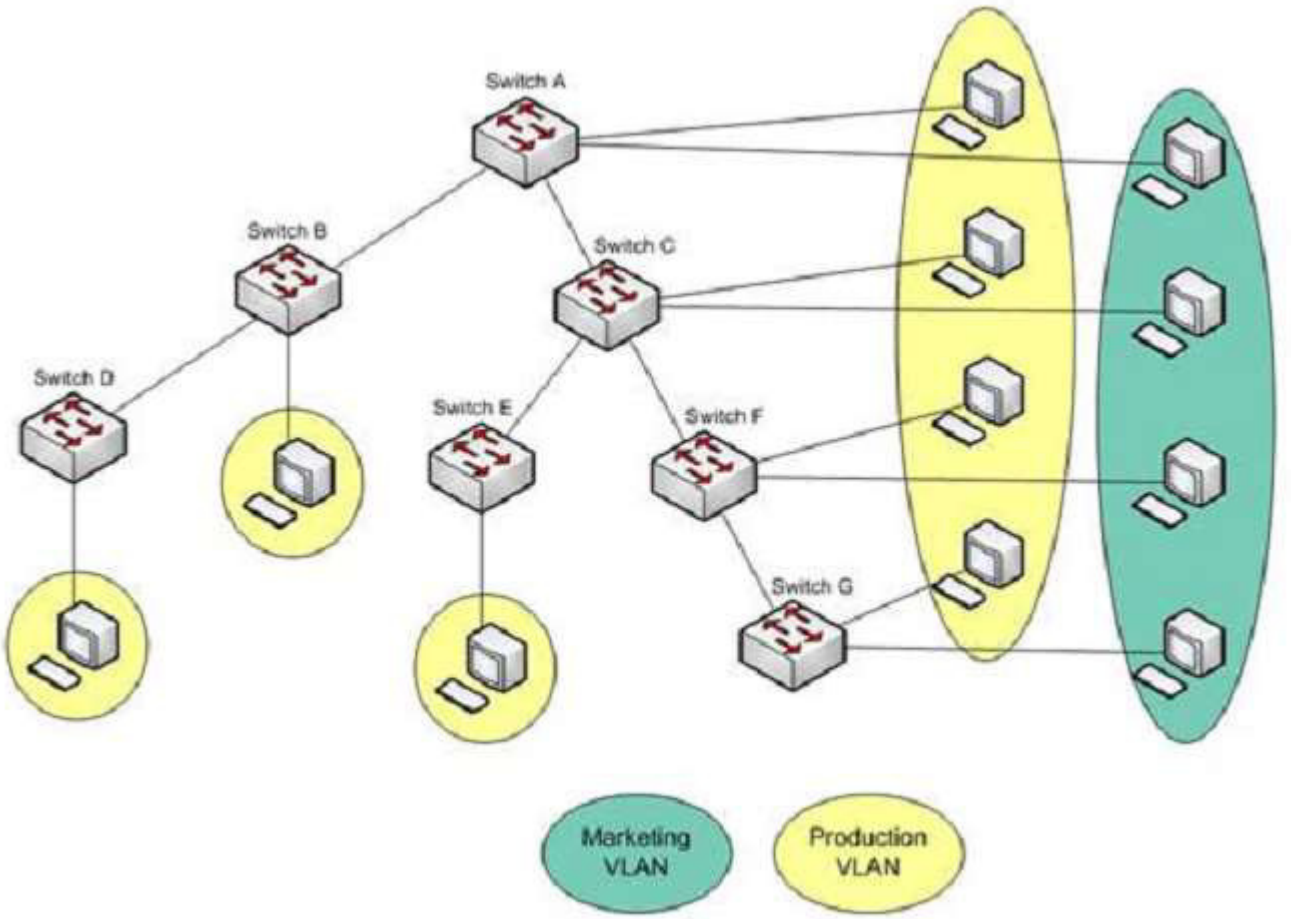
Objective:
LAN Switching Fundamentals

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

References:

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

QUESTION 98
You are a network administrator for your organization. Your organization has two Virtual LANs, named Marketing and Production. All switches in the network have both VLANs configured on them. Switches A, C, F, and G have user machines connected for both VLANs, whereas switches B, D, and E have user machines connected to the Production VLAN only. (Click the Exhibit(s) button to view the network diagram.)



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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

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

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

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

Objective:
Network Fundamentals

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

References:

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