vce trainer



Reference Solution for 200-301.vce

200-301

200-301

CCNA Cisco Certified Network Associate

Version 1.3

Score: 800/1000

Version:

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Exam A (455 questions)

Question 1

You have connected two routers in a lab using a Data Terminal Equipment (DTE)-to-Data Circuit-terminating Equipment (DCE) cable.

Which command must be issued on the DCE end for the connection to function?

- ☐ bandwidth
- ☐ no clock rate
- ☒ clock rate
- ☐ no bandwidth

Explanation:

Explanation:

You should issue the clock rate command on the DCE end for the connection to function. The clock rate is set on the Data Circuit-terminating Equipment (DCE) device. DCE is also known as Data Communications Equipment.

The DCE terminates a physical WAN connection, provides clocking and synchronization of a connection between two locations, and connects to a DTE. The DCE category includes equipment such as CSU/DSUs, NT1s, and modems. In the real world, the clock rate is provided by the CSU/DSU end at the telcom provider. In a lab, you must instruct the DCE end to provide a clock rate.

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

You would not issue the bandwidth command. This command is used to inform the router of the bandwidth of the connection for purposes of calculating best routes to locations where multiple routes exist. It is not necessary for the link described to function.

You should not issue the no clock rate command. This command is used to remove any previous settings implemented with the clock rate command.

You would not issue the no bandwidth command. This command is used to remove any previous settings implemented with the bandwidth command

Objective:

WAN Technologies

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco IOS Software Releases 11.1 > Configure > Feature Guides > Clock Rate Command Enhancements Feature Module

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 12: Point-to-Point WANs, pp. 446-447.

Question 2

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

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

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

- ☐ SwitchB(config-if)#switchport trunk vlan 15
- ☐ SwitchB(config)#switchport access vlan 15
- ☒ SwitchB(config-if)#switchport access vlan 15
- ☐ SwitchB(config-if)#switchport trunk vlan 15, 20

Explanation:

Explanation:

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

SwitchB(config)#interface fast 0/2

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

Licensed to Berend Post berend.post@it-university.nl

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

SwitchB(config-if)#switchport mode trunk

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Question 3

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

- ☒ split horizon
- ☐ poison reverse
- ☐ maximum hop count
- ☐ feasible successor

Explanation:

Explanation:

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

 Licensed to Berend Post berend.post@it-university.nl

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

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

To summarize this discussion:

Subinterfaces solve the NBMA split horizon issues.

There should be one IP subnet mapped to each DLCI

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco>Home>Support>Technology Support>IP>IP Routing>Technology Information>technology Whitepaper>EIGRP> Split Horizon and Poison Reverse

Question 4

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

- ☒ switch# show standby brief
- ☐ switch# show ip interface brief
- ☐ switch# show hsrp
- ☐ switch# show standby

Explanation:

Explanation:

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

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

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

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

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco > Cisco IOS IP Application Services Command Reference > show standby

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

Licensed to Berend Post berend.post@it-university.nl

Question 5

You are configuring Open Shortest Path First (OSPF) protocol for IPv6 on Router5. The router has two interfaces, which have been configured as follows:

S0/0 - 192.168.5.1/24
S0/1 - 10.0.0.6/8

You would like OSPF to route for IPv6 only on the S0/0 network. It should not route for IPv6 on the S0/1 network. The process ID you have chosen to use is 25. You do not want to apply an IPv6 address yet.

Which of the following command sets would enable OSPF for IPv6 as required?

- ☐ Router5(config)#ipv6 ospf 25
- ☐ Router5(config)# network 192.168.5.0
- ☐ Router5(config)#ipv6 ospf 25
- ☐ Router5(config)#router-id 192.168.5.1
- ☒ Router5(config)#ipv6 unicast-routing
- ☒ Router5(config)#ipv6 router ospf 25
- ☒ Router5(config-rtr)#router-id 1.1.1.1
- ☒ Router5(config)#interface S0/0
- ☒ Router5(config-if)#ipv6 ospf 25 area 0
- ☐ Router5(config)#ipv6 unicast-routing
- ☐ Router5(config)#ipv6 ospf 25
- ☐ Router5(config-rtr)#router-id 1.1.1.1

Explanation:

Explanation:

The correct command sequence would be as follows:

Router5(config)# ipv6 unicast-routing

Router5(config)# ipv6 router ospf 25

Router5(config-rtr)# router-id 1.1.1.1

Router5(config)# interface S0/0

Router5(config-if)# ipv6 ospf 25 area 0

The first line enables IPv6 routing with the ipv6 unicast-routing command. The second line enables OSPF routing for IPv6 with the ipv6 router ospf command. The third assigns a necessary router ID (which was chosen at random) with the router-id command. The last two lines enable OSPF for area 0 on the proper interface.

Licensed to Berend Post berend.post@it-university.nl

The following command set is incorrect because it does not enable OSPF routing for IPv6, assign a necessary router ID, or enable OSPF for area 0 on the proper interface:

Router5(config)# ipv6 ospf 25

Router5(config)# network 192.168.5.0

This command set also displays incorrect use of the network command. The network command would be used with OSPF v2.

The following command set fails to enable OSPF routing for IPv6, assign a necessary router ID, or enable OSPF for area 0 on the proper interface:

Router5(config)# ipv6 ospf 25

Router5(config)# router-id 192.168.5.1

It also assigns the router ID under global configuration mode, rather than under router ospf 25 configuration mode as required.

The following command set fails to enable OSPF for area 0 on the proper interface:

Router5(config)# ipv6 unicast-routing

Router5(config)# ipv6 ospf 25

Router5(config-rtr)# router-id 1.1.1.1

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Cisco > Implementing OSPF for IPv6 > How to Implement OSPF for IPv6

Cisco > Cisco IOS IPv6 Command Reference > ipv6 unicast-routing

Licensed to Berend Post berend.post@it-university.nl

Cisco > Cisco IOS IPv6 Command Reference > ipv6 ospf area

Question 6

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

- ☐ router(config-router)# line vty 0 4
- ☐ router(config-line)# login
- ☐ router(config-line)# password password
- ☐ router(config)# line telnet 0 4
- ☐ router(config-line)# login
- ☐ router(config-line)# password password
- ☐ router(config)# line aux 0
- ☐ router(config-line)# login
- ☐ router(config-line)# password password
- ☒ router(config)# line vty 0 4
- ☒ router(config-line)# login
- ☒ router(config-line)# password password

Explanation:

Explanation:

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

router(config)# line vty 0 4

router(config-line)# login

router(config-line)# password password

An explanation of the commands is below:

router(config)# line vty 0 4: Enters line configuration mode for virtual terminal lines 0 to 4.

router(config-line)# login: Ensures that any remote access is prompted for a password.

router(config-line)# password password: Sets a password of "password" for VTY lines.

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

Password required but not set

[Connection to foreign host 106.5.5.1 closed by foreign host]

Licensed to Berend Post berend.post@it-university.nl

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

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

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

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

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device management

References:

Cisco > Support > Technology Support > IP > IP Addressing Services > Design > Design TechNotes > Cisco Guide to Harden Cisco IOS Devices > Document ID: 13608

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

Licensed to Berend Post berend.post@it-university.nl

Question 7

Examine the partial output from two adjacent routers:

```
RTR78# show ip ospf
Routing Process 201 with ID 192.0.2.1 VRF default
 Stateful High Availability enabled
 Graceful-restart is configured
 Grace period: 60 state: Inactive
 Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an autonomous system boundary
Administrative distance 110
 Reference Bandwidth is 40000 Mbps
 Initial SPF schedule delay 3000.000 msecs,
 minimum inter SPF delay of 2000.000 msecs,
 maximum inter SPF delay of 4000.000 msecs
 Initial LSA generation delay 3000.000 msecs,

RTR79# show ip ospf
Routing Process 202 with ID 192.0.2.1 VRF default
 Stateful High Availability enabled
 Graceful-restart is configured
 Grace period: 60 state: Inactive
 Last graceful restart exit status: None
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an autonomous system boundary
Administrative distance 110
 Reference Bandwidth is 30000 Mbps
 Initial SPF schedule delay 3000.000 msecs,
 minimum inter SPF delay of 2000.000 msecs,
 maximum inter SPF delay of 4000.000 msecs
 Initial LSA generation delay 3000.000 msecs,
```

Which of the following statements describes why the two routers are NOT forming an OSPF neighbor adjacency?

- ☐ The process IDs do not match
- ☒ The router IDs are misconfigured
- ☐ The distance is misconfigured
- ☐ The reference bandwidth does not match

Explanation:

Explanation:

The output shows that the router IDs for RTR78 and RTR79 are the same value, which should not be the case. One of the two routers has been misconfigured with the other router's ID. This will prevent an OSPF neighbor adjacency from forming.

Other issues can that can prevent an adjacency are:

Mismatched OSPF area number

Licensed to Berend Post berend.post@it-university.nl

Mismatched OSPF area type

Mismatched subnet and subnet mask

Mismatched OSPF HELLO and dead timer values

The process IDs do not have to match. It does not matter whether they match or do not match because the process ID is only locally significant on the device.

The administrative distance is not misconfigured in the output. Both routers are using the default OSPF administrative distance of 110.

If the reference bandwidths do not match, it will affect the calculation of the path cost, but it will not prevent an adjacency from forming.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > OSPF Neighbor Problems Explained

Licensed to Berend Post berend.post@it-university.nl

Question 8

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

```
OldSwitch# show vtp status
VTP Version : 2
Configuration Revision : 62
Maximum VLANs supported locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Server
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
<output omitted>

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

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

- ☐ NewSwitch will delete its current VTP data.
- ☒ There will be 10 VLANs in the network.
- ☐ OldSwitch will retain its current VTP data.
- ☐ There will be 24 VLANs in the network.

Explanation:

Explanation:

If NewSwitch is introduced to the network, there will be 10 VLANs. The VLAN database of the new switch will overwrite the VLAN databases of the production switches because it is operating in server mode and has a higher VLAN configuration revision number.

VLAN Trunking Protocol (VTP) is used to synchronize VLANs between different switches. The VTP configuration revision number is used to determine which VTP switch has the most current version of the VLAN database, and is incremented whenever a VLAN change is made on a VTP server switch. The Configuration Revision: 125 output indicates that NewSwitch has a configuration revision number of 125, which will be compared to other switches in the same VTP domain, including OldSwitch, which has a revision number of 62. If the production switches have lower configuration revision numbers than the new switch, their VLAN databases will be replaced with the VLAN database of the new switch. Any switch ports that had been assigned to be removed from VLANs in the configuration database of the new switch will be disabled, possibly resulting in catastrophic

 Licensed to Berend Post berend.post@it-university.nl

network failure. All VTP switches in the same VTP domain should have a domain password defined, which will protect against a rogue switch being added to the network and causing VLAN database corruption.

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

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

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

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

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

Licensed to Berend Post berend.post@it-university.nl

Question 9

Which feature is NOT provided by flow control?

- ☐ buffering
- ☐ windowing
- ☒ full duplex transmission
- ☐ source-quench messaging

Explanation:

Explanation:

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

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

Controls the amount of data which the sender can send to the receiver.

Uses buffering, transmitting source-quench messages, and windowing to handle network congestion.

Determines the rate at which the data is transmitted between the sender and receiver.

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

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

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

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

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

Objective:

Licensed to Berend Post berend.post@it-university.nl

Network Fundamentals

Sub-Objective:

Compare and contrast OSI and TCP/IP models

References:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Internet Protocols > TCP

Question 10

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

- ☐ set port-security
- ☒ switchport port-security
- ☐ set port-security enable
- ☐ switchport port-security enable

Explanation:

Explanation:

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

switch(config-if)#switchport port-security

Switchport security can be used to:

Limit the computers that are allowed to connect to the LAN (by specifying the MAC addresses allowed on the port)

Limit the number of MAC address allowed to be accessing a port

Set the action the port will take when a violation of the security rule occurs

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

Objective:

Infrastructure Security

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

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

Question 11

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

- ☐ It connects different Internet Service Providers (ISPs).
- ☒ It can act as an address translator between the Internet and a local network.
- ☒ It conserves IP addresses.
- ☐ It creates additional IP addresses for the local network.
- ☒ It helps the local network connect to the Internet using unregistered IP addresses.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

References:

Question 12

Your assistant has been assigned the task of configuring one end of a WAN link between two offices. The link is a serial connection and the router on the other end is a non-Cisco router. The router in the other office has an IP address of 192.168.8.6/24. The connection will not come up, so you ask your assistant to show you the commands he configured on the Cisco router. The commands he executed are shown below.

Ciscorouter(config)# interface serial0/0
Ciscorouter(config-if)# ip address 192.168.8.5 255.255.255.0
Ciscorouter(config-if)# no shut

What command(s) should he run to correct the configuration?

- ☐ Ciscorouter(config-if)# no ip address 192.168.8.5
- ☐ Ciscorouter(config-if)# ip address 192.168.8.10
- ☒ Ciscorouter(config-if)# encapsulation ppp
- ☐ Ciscorouter(config-if)# encapsulation ansi
- ☐ Ciscorouter(config-if)# authentication chap

Explanation:

Explanation:

There are three encapsulation types available for a serial connection: High-Level Data Link Control (HDLC), Point-To-Point (PPP), and Frame Relay. HDLC is the default on Cisco routers and the form of HDLC used on a Cisco router is incompatible with routers from other vendors. Since the encapsulation command was not run, the router is set for HDLC. To correct this, you should execute the encapsulation ppp command. Frame Relay could also be used if the other router were running Frame Relay, since it also is an industry standard.

The IP address does not need to be changed. It is currently set for 192.168.8.5/24. This is correct since it is in the same subnet as the IP address of the other end,192.168.8.6/24.

The command authentication chap should not be run because the scenario does not indicate that authentication is configured on the other end. If it is set on one end, it must be set on the other as well.

The command encapsulation ansi should not be run because ANSI is not an encapsulation type. It is an LMI type used in Frame Relay. The three LMI options available are Cisco, ANSI, and ITU.

Objective:

Licensed to Berend Post berend.post@it-university.nl

WAN Technologies

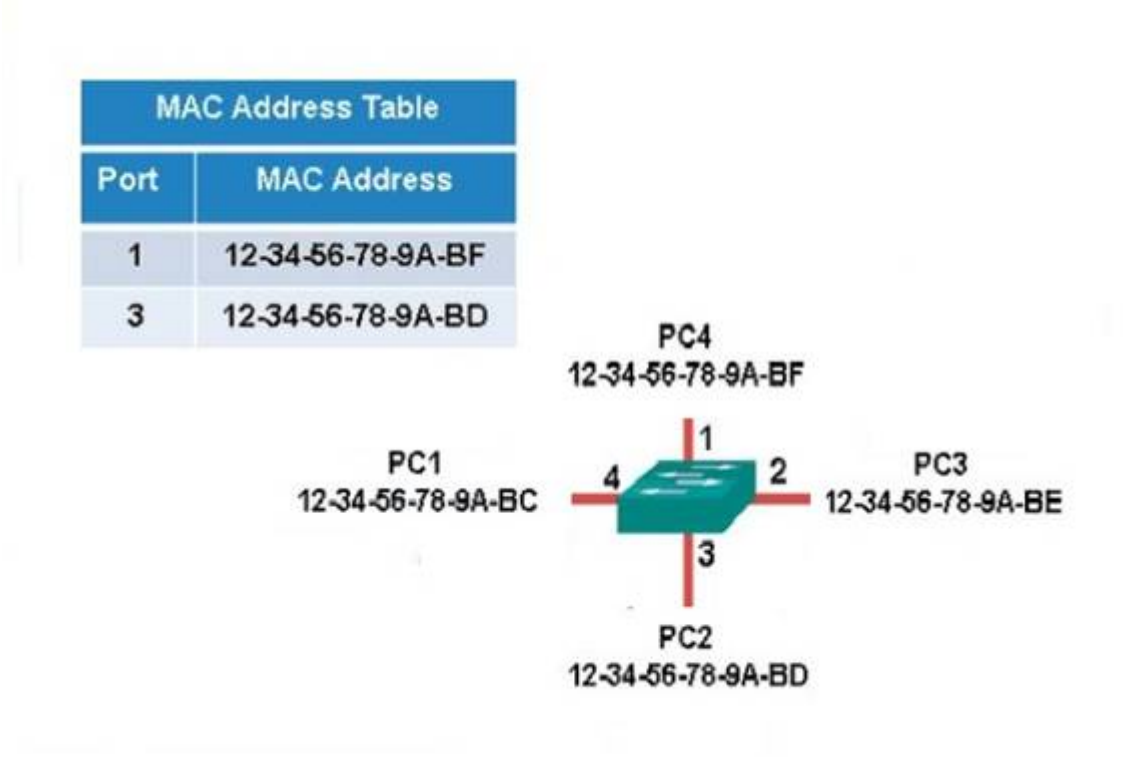
Sub-Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

Question 13

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



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

- ☐ source MAC: 12-34-56-78-9A-BD, destination MAC: 12-34-56-78-9A-BF
- ☐ source MAC: 12-34-56-78-9A-BF, destination MAC: 12-34-56-78-9A-BD
- ☒ source MAC: 12-34-56-78-9A-BF, destination MAC: 12-34-56-78-9A-BC
- ☐ source MAC: 12-34-56-78-9A-BC, destination MAC: 12-34-56-78-9A-BF

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Interpret Ethernet frame format

References:

Cisco Press > Articles > Cisco Certification > CCNA Routing and Switching > Basic Data Transmission in Networks: MAC Tables and ARP Tables

How do Switches Work?

Licensed to Berend Post berend.post@it-university.nl

Question 14

SwitchB receives a frame with the following fields:

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

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

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

How will SwitchB handle the frame it just received?

- ☐ It will forward the frame out all ports
- ☐ It will forward the frame out FastEthernet0/4 only
- ☐ It will drop the frame
- ☐ It will record the source MAC address
- ☒ It will forward the frame out FastEthernet0/10 only

Explanation:

Explanation:

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

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

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

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

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

Objective:

LAN Switching Fundamentals

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Describe and verify switching concepts

References:

Cisco Documentation > Internetworking Case Studies > LAN Switching

Question 15

Which metric does the Open Shortest Path First (OSPF) routing protocol use for optimal path calculation?

- ☐ MTU
- ☒ Cost
- ☐ Delay
- ☐ Hop count

Explanation:

Explanation:

OSPF is a link-state routing protocol which uses cost as a metric for optimal path calculation. It is an open standard protocol based on Dijkstra's Shortest Path First (SPF) algorithm. Metrics are used by routing protocols to determine the lowest cost path to a network number, which is considered the optimal or "fastest" path. Cisco's implementation of OSPF calculates the cost (metric) of a link as inversely proportional to the bandwidth of that interface. Therefore, a higher bandwidth indicates a lower cost, and a more favorable metric.

For this to work properly, the bandwidth of the link must be configured to allow OSPF to arrive at the cost of the link. This is done with the bandwidth command executed in interface configuration mode, and is entered in kbps. For example, if the link were 64 kbps, you would enter the following command:

Router(config-if)# bandwidth 64

The metric for any OSPF link defaults to 100,000,000/bandwidth. The bandwidth used in the formula is in bits per second. So, in this example the calculation would be 100,000,000 / 64000 = 1562.5. The cost assigned to the link would be 1562. The cost for a network route is the sum of all individual links in the path to that network.

If multiple paths are assigned equal costs, OSPF will load balance across the multiple paths. By default, it will limit this load balance to a maximum of four equal-cost paths. When this occurs, all

Licensed to Berend Post berend.post@it-university.nl

four equal-cost paths will be placed in the routing table. There are two approaches to allow or prevent load balancing when multiple equal cost paths are available:

Use the bandwidth command to make one or more of the paths either less or more desirable.

Use the ip ospf cost command to change the cost value assigned to one or more of the paths

Maximum Transmission Unit (MTU), bandwidth, delay, load, and reliability form a composite metric used by Interior Gateway Routing Protocol (IGRP) and Enhanced Interior Gateway Routing Protocol (EIGRP). IGRP is a distance vector routing protocol developed by Cisco Systems. Enhanced IGRP (EIGRP) is a Cisco-proprietary hybrid protocol having features of both distance-vector and link-state protocols.

Hop count is a metric used by Routing Information Protocol (RIP). The fewer hops between the routers, the better the path.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039

Cisco > Internetworking Technology Handbook > Open Shortest Path First (OSPF)

Question 16

Which Cisco Internetwork Operating System (IOS) command is used to view information about Open Shortest Path First (OSPF) routing processes?

- ☐ show ip ospf database
- ☐ show ip ospf statistics
- ☒ show ip ospf
- ☐ show ip ospf traffic

Explanation:

Explanation:

The show ip ospf command is used to view information about the OSPF routing processes. It does so by displaying the collection of link states present in the database. The syntax of the command is as follows:

Licensed to Berend Post berend.post@it-university.nl

Router# show ip ospf [process-id]

The process-id parameter of the command specifies the process ID. The output of the command is as follows:

```
Router# show ip ospf

Routing Process "ospf 203" with ID 21.0.0.1 and Domain ID 21.20.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 10 secs, Hold time between two SPFs 20 secs
Minimum LSA interval 10 secs. Minimum LSA arrival 5 secs
LSA group pacing timer 200secs
Interface flood pacing timer 110 msecs
Retransmission pacing timer 110 msecs
Number of external LSA 1. Checksum Sum 0x0
Number of opaque AS LSA 1. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 3. 1 normal 0 stub 1 nssa
External flood list length 0

Area BACKBONE(0)
Number of interfaces in this area is 4
Area has message digest authentication
SPF algorithm executed 6 times
Area ranges are
Number of LSA 3. Checksum Sum 0x29BEB
Number of opaque link LSA 1. Checksum Sum 0x0
Number of DCbitless LSA 3
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

The show ip ospf database command is incorrect because this command is used to view the OSPF database for a specific router.

The show ip ospf statistics command is incorrect because this command is no longer valid in IOS version 12.4.

The show ip ospf traffic command is incorrect because this command is no longer valid in IOS version 12.4.

Objective:

Routing Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

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

References:

Question 17

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

- ☐ boot config
- ☐ configuration-register edit
- ☒ config-register
- ☐ edit configuration-register

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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

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

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

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

Configuration register is 0x2102

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

Router#configure terminal

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

Router(config)#config

Router(config)#config-register 0x2142

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

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

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

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

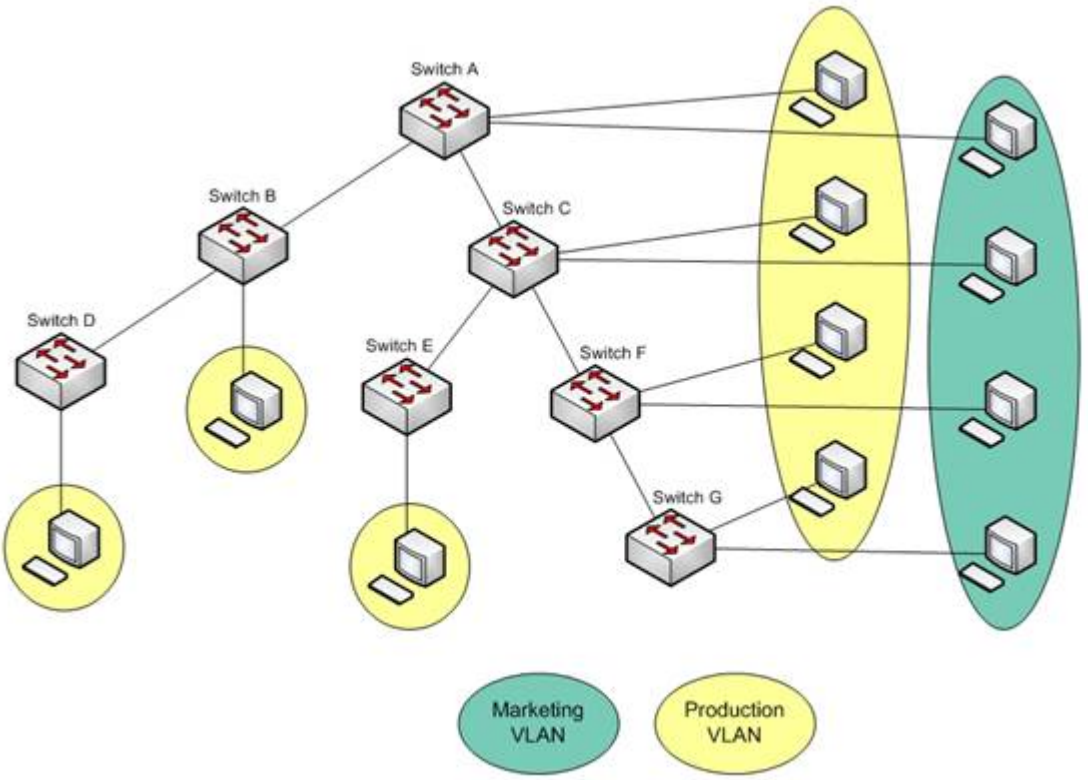
References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 18

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



To reduce broadcast traffic on the network, you want to ensure that broadcasts from the Marketing VLAN are flooded only to those switches that have Marketing VLAN users.

Which Cisco switch feature should you use to achieve the objective?

- ☐ PVST
- ☐ RSTP
- ☒ VTP Pruning
- ☐ Dynamic VLANs

Explanation:

Explanation:

The VLAN Trunking Protocol (VTP) pruning feature of Cisco VTP allows switches to dynamically delete or add VLANs to a trunk. It restricts unnecessary traffic, such as broadcasts, to only those switches that have user machines connected for a particular VLAN. It is not required to flood a frame to a neighboring switch if that switch does not have any active ports in the source VLAN. A trunk can also be manually configured with its allowed VLANs, as an alternative to VTP pruning.

Licensed to Berend Post berend.post@it-university.nl

All other options are incorrect because none of these features can be used to achieve the objective in this scenario.

The Per-VLAN Spanning Tree (PVST) feature allows a separate instance of Spanning Tree Protocol (STP) per VLAN. Each VLAN will have its own root switch and, within each VLAN, STP will run and remove loops for that particular VLAN.

Rapid Spanning Tree Protocol (RSTP) is an Institute of Electrical and Electronics Engineers (IEEE) standard. It reduces high convergence time that was previously required in STP implementations. It is interoperable with STP (802.1d).

With dynamic VLANs, the switch automatically assigns a switch port to a VLAN using information from the user machine, such as its Media Access Control (MAC) address or IP address. The switch then verifies information with a VLAN Membership Policy Server (VMPS) that contains a mapping of user machine information to VLANs.

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Cisco > Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.1E > Configuring VTP

Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design TechNotes > How LAN Switches Work > Document ID: 10607

Question 19

Which of the following characteristics are NOT shared by RIPv1 and RIPv2?

- ☐ They share an administrative distance value
- ☐ They use the same metric
- ☒ They both send the subnet mask in routing updates
- ☐ They have the same maximum hop count

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

RIPv1 and RIPv2 do NOT both send the subnet mask in routing updates. RIPv1 is classful, while RIPv2 is classless. This means the RIPv1 does not send subnet mask information in routing updates, while RIPv2 does.

Both versions have the same administrative distance of 120.

Both versions have the same metric, which is hop count.

Both versions have the same maximum hop count, which is 15.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Home > Knowledgebase > Cisco Certified Network Associate (CCNA) > Difference between RIPv1 and RIPv2

Cisco Press > Articles > Cisco Certification > CCDA > CCDA Self-Study: RIP, IGRP, and EIGRP Characteristics and Design

Question 20

You have implemented the following IP SLA configuration, as shown in the following partial output of the show run command:

ip sla 1
dns cow.cisco.com name-server 10.52.128.30
ip sla schedule 1 start-time now

Which of the following statements is true of this configuration?

- ☒ It will find the response time to resolve the DNS name cow.cisco.com
- ☐ It will find the response time to connect to the DNS server at 10.52.128.30
- ☐ It will start in one minute
- ☐ It will gather data from one minute

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

It will find the response time to resolve the DNS name cow.cisco.com. Domain Name System (DNS) response time is computed by calculating the difference between the time taken to send a DNS request and the time a reply is received. The Cisco IOS IP SLAs DNS operation queries for an IP address if the user specifies a hostname, or queries for a hostname if the user specifies an IP address.

It will not find the response time to connect to the DNS server at 10.52.128.30. That is the IP address of the DNS server being used for the operation (10.52.128.30). However, it will measure the response time to resolve the DNS name cow.cisco.com.

It will not start in one minute. It will start immediately, as indicated by the start-time now parameter.

It will not gather data for one minute. The numeral 1 in the first line refers to the IP SLA number, and the numeral 1 in the last line refers to the IP SLA number to be scheduled.

Objective:

Infrastructure Management

Sub-Objective:

Troubleshoot network connectivity issues using ICMP echo-based IP SLA

References:

Home > Support > Technology support > IP > IP application services > Technology information > Technology white paper > Cisco IOS IP Service Level Agreements User Guide

Question 21

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

- ☒ 192.24.134.127
- ☐ 192.24.134.128
- ☐ 192.24.134.129
- ☐ 192.24.134.131

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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

To subnet an existing network, you will use host bits to split the IP address into multiple logical subnets. For example, if you use three bits of the host ID for subnetting, you have created 23 = 2 x 2 x 2 = 8 subnets. Remaining bits of the host ID in decimal form will form the number of hosts on each subnet.

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

192.24.134.128 is the network ID for the next subnet created when using a mask of 255.255.255.128 on the class C network 192.24.134.0. The following network IDs are created when you use a mask of 255.255.255.128 on the class C network 192.24.134.0:

192.24.134.0 - Valid range 192.24.134.1-192.24.134.126, 192.24.134.127 is the broadcast

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

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

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 22

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

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

Explanation:

Explanation:

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

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

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

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

VPN solutions such as those supported by Cisco ASA firewalls and Cisco integrated routers provide the following benefits:

Lower desktop support costs

Threat protection

Flexible and cost-effective licensing

Reduced cost and management complexity

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

Licensed to Berend Post berend.post@it-university.nl

References:

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

Question 23

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

Ethernet 0/0 is up, line protocol is down

Which of the following can be determined from this output?

- ☒ the link is not functional due to a Data Link layer issue
- ☐ the link is fully functional
- ☐ the link is not functional due to a Physical layer issue
- ☐ the link is not functional due to both a Physical layer and a Data Link layer issue

Explanation:

Explanation:

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

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

Ethernet0/0 is up, line protocol is up

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

Ethernet 0/0 is down, line protocol is down

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

Objective:

LAN Switching Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

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

References:

Cisco > Support > Cisco IOS Interface and Hardware Component Command Reference > show interfaces

Question 24

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

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

- ☐ ICMP redirect
- ☐ ICMP time exceeded
- ☒ ICMP destination unreachable
- ☐ ICMP echo-reply

Explanation:

Explanation:

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

1. Network unreachable

2. Host unreachable

3. Protocol unreachable

4. Port unreachable

5. Fragmentation needed and Don't Fragment (DF) bit set

6. Source route failed

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 25

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

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

- ☐ enable password griswald
- ☐ hostname R1
- ☐ username R1 password poppycock
- ☐ interface serial 0/0
- ☐ ip address 192.168.5.5 255.255.255.0
- ☐ encapsulation ppp
- ☐ ppp authentication chap
- ☐ enable password griswald
- ☐ hostname R1
- ☐ username R1 password poppycok
- ☐ interface serial 0/1
- ☐ ip address 192.168.5.5 255.255.255.0
- ☐ encapsulation ppp
- ☐ ppp authentication chap
- ☒ enable password griswald
- ☒ hostname R1
- ☒ username R2 password poppycock
- ☒ interface serial 0/0
- ☒ ip address 192.168.5.5 255.255.255.0
- ☒ encapsulation ppp
- ☒ ppp authentication chap
- ☐ enable password griswald
- ☐ hostname R1
- ☐ username R1 password griswald
- ☐ interface serial 0/0
- ☐ ip address 192.168.5.5 255.255.255.0
- ☐ encapsulation ppp
- ☐ ppp authentication chap

Explanation:

Explanation:

The correct configuration is as follows:

enable password griswald

hostname R1

username R2 password poppycock

interface serial 0/0

Licensed to Berend Post berend.post@it-university.nl

ip address 192.168.5.5 255.255.255.0

encapsulation ppp

ppp authentication chap

The key settings that are common problems are as follows:

The username is set to the hostname of the other router (in this case, R2)

The password is set poppycock which must be the same in both routers

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

enable password griswald

hostname R1

username R1 password poppycock

interface serial 0/0

ip address 192.168.5.5 255.255.255.0

encapsulation ppp

ppp authentication chap

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

enable password griswald

hostname R1

username R1 password poppycok

interface serial 0/0

ip address 192.168.5.5 255.255.255.0

encapsulation ppp

ppp authentication chap

Licensed to Berend Post berend.post@it-university.nl

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

enable password griswald

hostname R1

username R1 password griswald

interface serial 0/0

ip address 192.168.5.5 255.255.255.0

encapsulation ppp

ppp authentication chap

Objective:

WAN Technologies

Sub-Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

Cisco > Home > Support > Technology Support > WAN > Point-to-Point Protocol (PPP) > Design > Design TechNotes > Understanding and Configuring PPP CHAP Authentication

Question 26

Multiple routes to a destination already exist from various routing protocols.

Which of the following values is used FIRST to select the route that is inserted into the route table?

- ☐ composite metric
- ☒ administrative distance
- ☐ prefix length
- ☐ hop count

Explanation:

Explanation:

When multiple routes to a destination exist from various routing protocols, the first value to be evaluated is the administrative distance of the source of the route. The following are examples of default administrative distance values:

Licensed to Berend Post berend.post@it-university.nl

Connected	0
Static	1
eBGP	20
EIGRP(internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP(external)	170
iBGP	200
EIGRP summary route	5

The second value to be compared is the composite metric, or any metric value for that matter. It is only used when multiple routes exist that have the same administrative distance.

The prefix length is only used to compare two existing routes in the routing table that lead to the destination, yet have different mask or prefix lengths. In that case, the route with the longest prefix length will be chosen.

Hop count is ONLY used when comparing multiple RIP routes. It is not the first consideration when multiple routes from various routing protocols exist in a routing table.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Configuration Example and TechNotes > Route Selection in Cisco Routers

Licensed to Berend Post berend.post@it-university.nl

Question 27

The conference room has a switch port available for use by the presenter during classes. Each presenter uses the same PC attached to the port. You would like to prevent any other PCs from using that port. You have completely removed the former configuration in order to start anew.

Which of the following steps are required to prevent any other PCs from using that port?

- ☐ make the port a trunk port
- ☒ enable port security
- ☒ make the port an access port
- ☒ assign the MAC address of the PC to the port
- ☐ make the port a sticky port
- ☐ set the maximum number of MAC addresses on the port to 1

Explanation:

Explanation:

You should create the port as an access port, enable port security, and statically assign the MAC address of the PC to the port. Creating the port as an access port ensures that the PC can use the port and port security can be enabled on the port. The second step is to enable port security, which is required to use the third command. The third command sets the MAC address of the PC as the statically assigned address on that port, meaning that only that address can send and receive on the port.

You should not make the port a trunk port. There is no need to make this a trunk port because it will not be carrying multiple VLAN traffic, only the traffic of the PC.

You should not make the port a sticky port. The sticky keyword, when used with switchport port-security command, is used to allow a port to dynamically learn the first MAC address it sees in the port, add it to the MAC address table, and save it to the running configuration of the switch. It will not limit the MAC addresses allowed on the port to that of the PC.

You should not set the maximum number of MAC addresses on the port to 1. That would prevent the attachment of a hub or switch to the port, but would not restrict the MAC addresses allowed on the port to the MAC address of the PC.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot port security

Licensed to Berend Post berend.post@it-university.nl

References:

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA > Configuring Port Security

Question 28

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

- ☐ ICMP can identify network problems.
- ☐ ICMP is documented in RFC 792.
- ☒ ICMP provides reliable transmission of data in an Internet Protocol (IP) environment.
- ☐ An ICMP echo-request message is generated by the ping command.

Explanation:

Explanation:

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

The following statements are TRUE regarding ICMP:

ICMP can identify network problems.

ICMP is documented in RFC 792.

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

An ICMP echo-reply message is an indicator that the destination node is reachable.

ICMP is a network-layer protocol that uses message packets for error reporting and informational messages.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast TCP and UDP protocols

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 29

Which of the following is NOT a packet type used by Enhanced Interior Gateway Routing Protocol (EIGRP)?

- ☐ Query
- ☐ Reply
- ☐ Ack
- ☒ Response

Explanation:

Explanation:

Response is not a packet type used by EIGRP. The following are the packet types used by EIGRP:

Hello/Ack: Establish neighbor relationships. The Ack packet is used to provide acknowledgement of a reliable packet.

Update: Send routing updates.

Query: Ask neighbors about routing information.

Reply: Provide response to queries about routing information.

Requests: Gain specific information from one or more neighbors.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Cisco > Support > Cisco IOS Software > Configuring EIGRP

Question 30

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

- ☒ 192.168.54.0
- ☐ 192.168.54.8
- ☐ 192.168.54.4
- ☐ 192.168.54.16

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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

192.168.54.0

192.168.54.32

192.168.54.64

192.168.54.92 and so on.

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

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

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

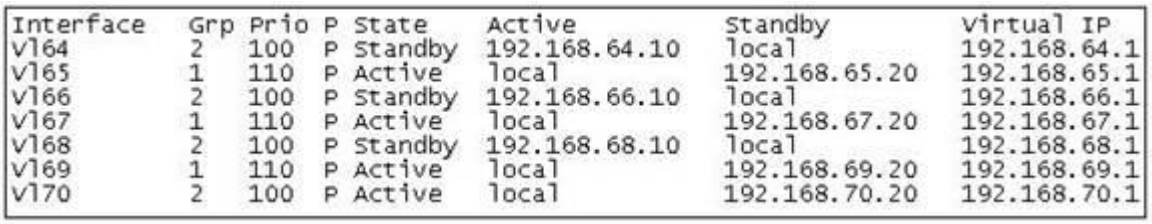
References:

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

 Licensed to Berend Post berend.post@it-university.nl

Question 31

What command would provide the output displayed in the exhibit? (Click on the Exhibit(s) button.)



Interface	Grp	Prio	P	State	Active	Standby	Virtual IP
Vl64	2	100	P	Standby	192.168.64.10	local	192.168.64.1
Vl65	1	110	P	Active	local	192.168.65.20	192.168.65.1
Vl66	2	100	P	Standby	192.168.66.10	local	192.168.66.1
Vl67	1	110	P	Active	local	192.168.67.20	192.168.67.1
Vl68	2	100	P	Standby	192.168.68.10	local	192.168.68.1
Vl69	1	110	P	Active	local	192.168.69.20	192.168.69.1
Vl70	2	100	P	Active	local	192.168.70.20	192.168.70.1

- ☐ switch# show hsrp
- ☐ switch# show standby
- ☐ switch# show interface vlan
- ☒ switch# show standby brief

Explanation:

Explanation:

The command show standby brief displays the output in the exhibit. It is used to display a summary of the HSRP groups of which the switch is a member. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. In the exhibit, the interface VLAN 64 is a member of HSRP group 2. Its priority in the group is 100 and it is currently the standby switch. Since preemption is configured (as indicated by the P following the priority), we know that the priority of this switch must be lower than the priority of the active device. The active device has an IP address of 192.168.64.10 and the group IP address is 192.168.64.1.

The command show standby can be used to display detailed information about HSRP groups of which a switch is a member. It does not provide the quick summary display of the exhibit. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch. The command syntax is show standby [type number [group]].

Below is an example of this command's output:

Licensed to Berend Post berend.post@it-university.nl

```
RouterA#show standby vlan 5

VLAN 5 - group 1
Local state is Active, priority 105, may preempt
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.10 configured
Active router is local
Standby router is 192.12.23.3 expires in 9.600
Virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:01:38
<output omitted>

VLAN 5- group 2
Local state is Standby, priority 100
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.11 configured
Active router is 192.168.23.3 expires in 9.600
Standby router is local
2 state changes, last state change 00:01:38
<output omitted>
```

In the above output, Router A is load-sharing traffic for VLAN 5. It is active for group 1 and standby for group 2. The router at address 192.168.23.3 is active for group 2 and standby for group 1. This allows traffic to be sent to both routers while still allowing for redundancy. Router A was also configured with the standby 1 preempt command (results seen in line 1), which allows it to resume its role as active for group 1 if it comes back up from an outage.

The command show interface vlan is not a complete command. A VLAN number must follow the command. When provided with a VLAN number, the output would display the status of the SVI, but no HSRP information.

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

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco > Cisco IOS IP Application Services Command Reference > show standby through show udp > show standby

Licensed to Berend Post berend.post@it-university.nl

Question 32

Which Cisco IOS command would prompt for input in the following format?

```
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.142.23.10
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort
```

- ☐ ping 10.1.1.1
- ☒ ping
- ☐ traceroute
- ☐ tracert

Explanation:

Explanation:

The extended ping command prompts the user for input in the format given in this scenario. The extended ping command is accessed by issuing a ping command without specifying an IP address. This causes the ping command to transit into extended ping command mode, where you can specify and modify various parameters, such as packet size, timeout, and repeat count.

The following code is a sample partial output of the extended ping command:

```
Router A#ping
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.142.23.10
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```


Licensed to Berend Post berend.post@it-university.nl

The true value of the extended ping command lies in the ability to ping FROM a different device than the one you are working from. As shown in the above output, you can specify the source address on line 8.

The ping 10.1.1.1 command is incorrect because it sends an ICMP "echo request" to the target host. In turn, the target host replies with the "echo reply" packets. When pinging from one device to another on the network, ICMP and Address Resolution Protocol (ARP) are used. ARP resolves an IP address to its associated MAC addresses.

The tracert command is incorrect because this command is used by Microsoft Windows, not Cisco. It is not a valid utility to run via the Cisco IOS command-line interface. The tracert command is similar to the traceroute Cisco utility as the tracert command tests the connectivity or "reachability" of a network device or host. It reports back a reply at each hop, allowing one to determine where the communication link is "broken".

The traceroute command is used to display the path that a packet follows to its destination. This command displays the IP address of each router in the path from the source to the destination address. Unlike the Microsoft tracert command, which uses the ICMP protocol, the Cisco traceroute command is based on User Datagram Protocol (UDP). The following code is the partial output of the traceroute command.

RouterA#traceroute 124.10.23.41

Type escape sequence to abort.

Tracing the route to 124.10.23.41

1 121.10.1.3 6 msec 6 msec 6 msec

2 134.10.10.13 30 msec 17 msec 14 msec

3 32.1.2.4 36 msec * 23 msec

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730

Cisco > Tech Notes > Understanding the Ping and Traceroute Commands > The Traceroute Command > Document ID: 12778

Question 33

Which type of Dynamic Host Configuration Protocol (DHCP) transmission is used by a host to forward a DHCPDISCOVER packet to locate a DHCP server on the network?

- ☐ unicast
- ☒ broadcast
- ☐ multicast
- ☐ anycast

Explanation:

Explanation:

Hosts broadcast DHCPDISCOVER messages to locate a DHCP server. The following steps are followed during the allocation of the IP address dynamically using a DHCP server:

The client device broadcasts a DHCPDISCOVER message to locate a DHCP server.

The DHCP server replies with a DHCPOFFER unicast message with configuration parameters, such as an IP address, a MAC address, a domain name, and a lease for the IP address for the client device.

The client returns a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the DHCP server.

The DHCP server replies to client device with DHCPACK unicast message, acknowledging the allocation of the IP address to this client device.

Dynamic Host Configuration Protocol (DHCP) is an enhancement over Bootstrap Protocol (BOOTP) and is used to automate the distribution of IP address to clients from a central server. BOOTP protocol was also used to distribute IP addresses, but was inflexible to changes in the network.

DHCP offers the following three advantages that also addressed the inflexibility of the BOOTP protocol:

Automatic allocation of permanent IP addresses

Automatic allocation of time bound (leased) IP addresses

Provision of assigning static IP address or defining a pool of reserved IP address

DHCP does not use multicast messages.

Licensed to Berend Post berend.post@it-university.nl

Anycast is a concept of IPv6 protocol and is not valid type used by DHCP.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify DHCP on a router (excluding static reservations)

References:

Cisco > Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 > Part 3: DHCP > DHCP Server, Relay Agent, and Client Operation

Question 34

In the given exhibit, which combination shows the components of a bridge ID used for Spanning Tree Protocol (STP)?

1

VLAN Number	MAC Address

2

Priority Number	Serial Number

3

Priority Number	MAC Address

4

VLAN Number	Serial Number

- ☐ 1
- ☐ 2
- ☒ 3
- ☐ 4

Explanation:

Explanation:

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

Switch's priority number: Configured as 32768 on Cisco switches by default

Licensed to Berend Post berend.post@it-university.nl

Switch's Media Access Control (MAC) address: The burnt-in hardware address of the network interface card (NIC)

The switch with the lowest bridge ID is elected as the root bridge. If the same priority number is configured on two or more switches in the network, the switch with the lowest MAC address will become the root.

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

The combinations of the remaining options are incorrect because Virtual LAN (VLAN) numbers and serial numbers are not components of a bridge ID.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco Documentation > Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX > Configuring STP and IEEE 802.1s MST > Understanding the Bridge IDCCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot STP protocols

Licensed to Berend Post berend.post@it-university.nl

Question 35

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

- ☐ Root port
- ☒ Backup port
- ☒ Alternate port
- ☐ Designated port
- ☐ Learning port

Explanation:

Explanation:

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

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

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

A designated port is the port used by a network segment to reach the root switch. Designated ports lead away (downstream) from the root switch, and are determined by the lowest path cost to the root switch. While a switch can only have one root port, every other port could potentially be a designated port. Whenever a network segment could be serviced by more than one switch, STP will elect one switch as designated for the segment, and the other(s) will be blocking. This is a core function of the STP protocol, in that only one active Layer 2 path can exist between any two network segments. This port type is available in STP.

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

Objective:

LAN Switching Fundamentals

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure, verify, and troubleshoot STP-related optional features

References:

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

Question 36

What command would be used to verify trusted DHCP ports?

- ☐ show mls qos
- ☒ show ip dhcp snooping
- ☐ show ip trust
- ☐ show ip arp trust

Explanation:

Explanation:

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

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

DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP snooping can be used to determine what ports are able to send DHCP server packets, such as DHCPOFFER, DHCPACK, and DHCPNAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

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

The other commands are incorrect because they have invalid syntax.

Objective:

Infrastructure Security

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Describe common access layer threat mitigation techniques

References:

Cisco > Cisco IOS IP Addressing Services Command Reference > DHCP Commands > show ip dhcp snooping

Question 37

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

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

- ☐ 300 workstations in a single broadcast domain, each workstation in its own collision domain
- ☒ 300 workstations, with 150 workstations in two broadcast domains and each workstation in its own collision domain
- ☐ 300 workstations, with 150 workstations in two broadcast domains and all workstations in the same collision domain
- ☐ 600 workstations, with 300 workstations in two broadcast domains and each workstation in its own collision domain

Explanation:

Explanation:

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

References:

Cisco Documentation > Internetwork Design Guide > Internetworking Basics

Question 38

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

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

- ☐ The route with an R next to it
- ☐ The route with an S next to it
- ☒ The route with a C next to it
- ☐ The route with an I next to it

Explanation:

Explanation:

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

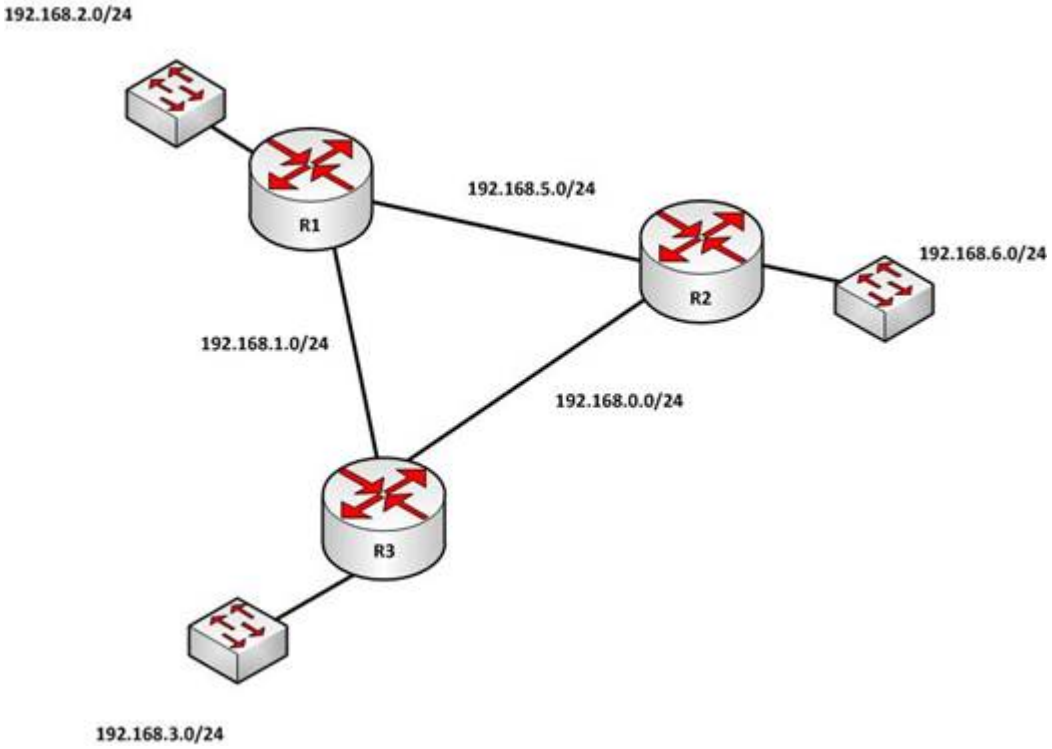
It is significant to note that routers with no static routes and no routing protocols enabled will populate all directly connected routes to the routing table with no action on the part of the administrator. Routes that are NOT directly connected will not be in the routing table unless one of two things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

Licensed to Berend Post berend.post@it-university.nl

A static route is created by the administrator

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

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



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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Cisco > Support > IP > IP Addressing Services > Design Technotes > What Is Administrative Distance? > Document ID: 15986

Question 39

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

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

- ☒ ICMP path echo operation
- ☐ Internet Control Message Protocol Echo Operation
- ☐ UDP Jitter Operation for VoIP
- ☐ UDP Jitter Operation

Explanation:

Explanation:

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Infrastructure Management

Sub-Objective:

Troubleshoot network connectivity issues using ICMP echo-based IP SLA

References:

Home > Support > Technology support > IP > IP application services > Technology information > Technology white paper > Cisco IOS IP Service Level Agreements User Guide

Question 40

When the auth keyword is used in the snmp-server host command, which of the following must be configured with an authentication mechanism?

- ☐ the interface
- ☐ the host
- ☒ the user
- ☐ the group

Explanation:

Explanation:

The auth keyword specifies that the user should be authenticated using either the HMAC-MD5 or HMAC-SHA algorithms. These algorithms are specified during the creation of the SNMP user.

For example, the following command creates a user named V3User who will be a member of the SNMP group V3Group and will use HMAC-MD5 with a password of Password:

snmp-server user V3User V3Group v3 auth md5 Password

The authentication mechanism is not configured on the interface. All SNMP commands are executed at the global configuration prompt.

The authentication mechanism is not configured at the host level. The version and security model (authentication, authentication and encryption, or neither) are set at the host level.

Licensed to Berend Post berend.post@it-university.nl

The authentication mechanism is not configured at the SNMP group level. The group level is where access permissions like read and write are set. This is why a user account must be a member of a group to derive an access level, even if it is a group of one.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device-monitoring protocols

References:

Configuring SNMP Support > Understanding SNMP > SNMP Versions

Cisco IOS Network Management Command Reference > snmp-server engineID local through snmp trap link-status > snmp-server host

Question 41

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

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

- ☐ ssh
- ☒ telnet
- ☐ terminal
- ☐ virtual

Explanation:

Explanation:

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

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

The following parameters are used with the telnet command:

hostname: Specifies the name of the host.

interface_name: Specifies the name of the network interface to which you need to telnet.

Licensed to Berend Post berend.post@it-university.nl

IP_address: Specifies the IP address of the host.

IPv6_address: Specifies the IPv6 address associated to the host.

timeout number: Specifies the number of minutes that a telnet session can be idle.

The following features are the key characteristics of Telnet:

It is a client server protocol.

It uses TCP port number 23.

It is used to establish a remote connection over the internet or Local Area Network (LAN).

Telnet does not encrypt any data sent over the connection; that is, the data travels in clear text.

A Cisco router supports five simultaneous telnet sessions, by default. These lines are called vty 0-4.

A successful Telnet connection requires that the destination device be configured to support Telnet connections, which means it must be configured with a Telnet password.

The telnet command can also be used to test application layer connectivity to a device.

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

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

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

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device management

References:

Cisco > Cisco IOS Terminal Services Command Reference > telnet

Licensed to Berend Post berend.post@it-university.nl

Question 42

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?

- ☐ Inside local address
- ☐ Outside local address
- ☒ Inside global address
- ☐ Outside global address

Explanation:

Explanation:

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

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

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

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

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot inside source NAT

References:

Cisco > Support > Technology Support > IP > IP Addressing Services > Design > Design TechNotes > NAT: Local and Global Definitions

Cisco > Articles > Network Technology > General Networking > Network Address Translation

Licensed to Berend Post berend.post@it-university.nl

Question 43

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

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

Explanation:

Explanation:

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

It is a twisted-pair copper wire cable.

The RJ-45 connectors at both ends have the same conductor arrangement.

It is also known as a patch cable.

You can connect a switch to a router using a straight-through cable.

You can connect a router to a hub or a workstation to a hub using a straight-through cable.

All the other options are incorrect because they are the characteristics of a crossover cable.

Objective:

Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 44

When executed on a HSRP group member named Router 10, what effect does the following command have?

Router10(config-if)# standby group 1 track serial0 25

- ☐ It will cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down
- ☐ It will cause the router to shut down the Serial0 interface if 25 packets have been dropped
- ☐ It will cause the router to notify Router 25 is serial 0 goes down
- ☒ It will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down

Explanation:

Explanation:

This command will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down. Interface tracking can be configured in Hot Standby Routing Protocol (HSRP) groups to switch traffic to the standby router if an interface goes down on the active router. This is accomplished by having the active router track its interface. If that interface goes down, the router will decrement its HSRP priority by the value configured in the command. When properly configured, this will cause the standby router to have a higher HSRP priority, allowing it to become the active router and to begin serving traffic.

When the standby router in an HSRP group is not taking over the active role when the active router loses its tracked interface, it is usually a misconfigured decrement value, such that the value does not lower the HSRP priority of the active router far enough for the standby to have a superior priority value.

The command will not cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down. HSRP routers track their own interfaces, not those of another router.

The command will not cause the router to shut down the Serial0 interface if 25 packets have been dropped. It will only do this if the link becomes unavailable.

The command will not cause the router to notify Router 25 is serial 0 goes down. The number 25 in the command is the decrement value, not the ID of another router.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands

Cisco > Cisco IOS IP Application Services Command Reference > standby track

Question 45

Given the following output, which statements can be determined to be true? (Choose three.)

RouterA2# show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
192.168.23.2 1 FULL/BDR 00:00:29 10.24.4.2 FastEthernet1/0
192.168.45.2 2 FULL/BDR 00:00:24 10.1.0.5 FastEthernet0/0
192.168.85.1 1 FULL/- 00:00:33 10.6.4.10 Serial0/1
192.168.90.3 1 FULL/DR 00:00:32 10.5.5.2 FastEthernet0/1
192.168.67.3 1 FULL/DR 00:00:20 10.4.9.20 FastEthernet0/2
192.168.90.1 1 FULL/BDR 00:00:23 10.5.5.4 FastEthernet0/1
<<output omitted>>

- ☐ This router is the DR for subnet 10.1.0.0.
- ☒ The DR for the network connected to Fa0/0 has an interface priority greater than 2.
- ☐ The DR for the network connected to Fa0/1 has a router ID of 10.5.5.2.
- ☐ The DR for the serial subnet is 192.168.85.1.
- ☒ This router is neither the DR nor the BDR for the Fa0/1 subnet.
- ☒ RouterA2 is connected to more than one multi-access network.

Explanation:

Explanation:

The show ip ospf neighbor command displays a list of all OSPF routers with which you have established a neighbor relationship. The following describes the command output:

Neighbor ID: the Router ID (RID) of the neighboring router

Pri: the interface priority of the neighboring router, which is used to determine which router should serve the function of a Designated Router (DR)

State: the functional state of the neighboring router

Dead Time: the period that the router will wait to hear a Hello packet from this neighbor before declaring the neighbor down

Address: the IP address of the neighboring router on this subnet

Interface: the local interface over which the neighbor relationship (adjacency) was formed

The output for neighbor 192.168.45.2 is as follows:

 Licensed to Berend Post berend.post@it-university.nl

192.168.45.2 2 FULL/BDR 00:00:24 10.1.0.5 FastEthernet0/0

This indicates that the interface priority of neighbor 192.168.45.2 is 2. The default OSPF interface priority is 1, and the highest interface priority determines the designated router (DR) for a subnet. This same line reveals that this neighbor is currently the backup designated router (BDR) for this segment, which indicates that another router became the DR. It can be then be assumed that the DR router has an interface priority higher than 2. (The router serving the DR function is not present in the truncated sample output.)

The output for the two neighbors discovered on F0/1 is as follows:

192.168.90.3 1 FULL/DR 00:00:32 10.5.5.2 FastEthernet0/1

192.168.90.1 1 FULL/BDR 00:00:23 10.5.5.4 FastEthernet0/1

This output indicates that router 192.168.90.3 is the DR, and router 192.168.90.1 is the BDR for this network. Since there can only be one DR and BDR per segment, this indicates that the local router is neither the DR nor the BDR. (OSPF considers these DROther routers.)

The fact that multiple DRs are listed in this output indicates that RouterA2 is connected to more than one multi-access segment, since each segment will elect a DR.

It cannot be determined if this router is the DR for subnet 10.1.0.0. The output indicates that router 192.168.45.2 is the BDR for this network, but with the truncated output, it cannot be determined if this router is the DR.

The DR for the network connected to Fa0/1 does not have a router ID of 10.5.5.2. The Address field of the show ip ospf neighbor command indicates the IP address of the neighbor's interface, not the router ID of the neighbor.

The DR for the serial subnet is not 192.168.85.1, since point-to-point serial interfaces do not elect DRs and BDRs. This is indicated by the output below:

192.168.85.1 1 FULL/- 00:00:33 10.6.4.10 Serial0/1

Objective:

Routing Fundamentals

Sub-Objective:

 Licensed to Berend Post berend.post@it-university.nl

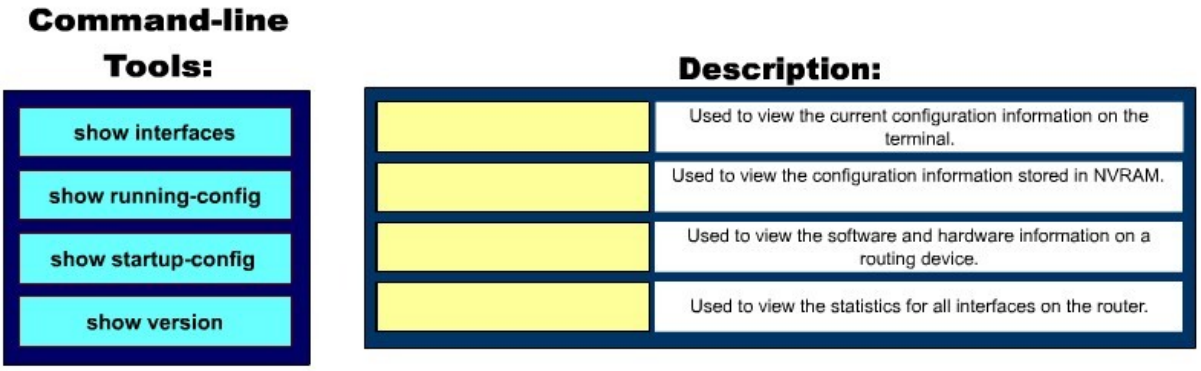
Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

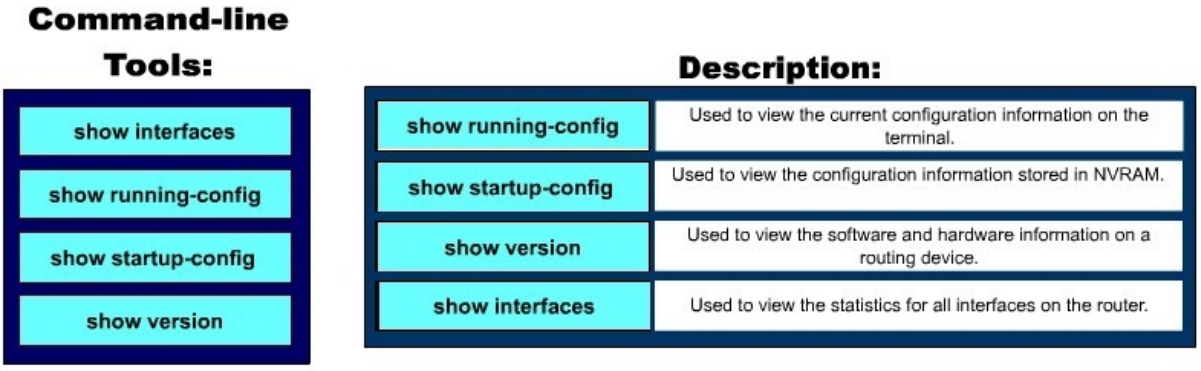
Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039 > DR Election

Question 46

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



Solution:



Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl

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 Management

Sub-Objective:

Perform device maintenance

References:

Cisco Documentation > Cisco IOS Configuration Fundamentals Command Reference, Release 12.4 > show running-config through showmon

Question 47

Which of the following commands configures an SNMP host to authenticate a user by username and send clear text notifications, the receipt of which will be acknowledged by the receiver?

- ☒ Router(config)# snmp-server host 192.168.5.5 informs version 3 noauth public
- ☐ Router(config)# snmp-server host 192.168.5.5 traps version 3 auth public
- ☐ Router(config)# snmp-server host 192.168.5.5 informs version 2c public
- ☐ Router(config)# snmp-server host 192.168.5.5 informs version 3 authpriv public

Explanation:

Explanation:

The command snmp-server host 192.168.5.5 informs version 3 noauth CISCO will configure the host to authenticate a user by username and send clear text notifications. The receiver will then acknowledge receipt of the notification. The keyword informs indicates that an inform message type will be used. Unlike a trap, an inform message is acknowledged by the receiver.

The version 3 keyword indicates that version 3 is in use, which is the ONLY version that supports authentication and encryption. Finally, the noauth keyword specifies authentication by username only and no encryption.

The command snmp-server host 192.168.5.5 traps version 3 auth public configures the host to send traps rather than informs.

Licensed to Berend Post berend.post@it-university.nl

The command snmp-server host 192.168.5.5 informs version 2c public specifies version 2c, which only support community string-based authentication.

The command snmp-server host 192.168.5.5 informs version 3 authpriv public specifies the keyword authpriv, which indicates encryption will be used and authentication based on HMAC-MD5 or HMAC-SHA algorithms.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device-monitoring protocols

References:

Configuring SNMP Support > Understanding SNMP > SNMP VersionsCisco IOS Network Management Command Reference > snmp-server engineID local through snmp trap link-status > snmp-server host

Question 48

You need to set the Telnet password to "john" on a Cisco router. Which set of commands would you use?

- ☒ Router(config)#line vty 0 4
- ☒ Router(config-line)#login
- ☒ Router(config-line)#password john
- ☐ Router(config)#line con 0
- ☐ Router(config-line)#login
- ☐ Router(config-line)#password john
- ☐ Router(config)#line vty 0 4
- ☐ Router(config-line)#login
- ☐ Router(config-line)#enable secret john
- ☐ Router(config)#line con 0
- ☐ Router(config-line)#login
- ☐ Router(config-line)#enable password john

Explanation:

Explanation:

The set of commands which would be used to configure the Telnet password to "john" on a Cisco router is:

Router(config)#line vty 0 4

Licensed to Berend Post berend.post@it-university.nl

Router(config-line)#login

Router(config-line)#password john

The line vty command is used to configure the router to enable Telnet access. By using this command, the router can be configured to accept one or more Telnet sessions.

The login and password parameters are the line configuration commands used to configure the password. The password command specifies the password and the login command instructs the router to require the password. By default, the login parameter is present in the configuration of the VTY lines. Because its presence indicates that a password is required for connecting to the VTY lines, if a password has not been configured on the VTY lines, a connection cannot be made. If an attempt were made to connect to the VTY line with the login parameter in effect and no password present, the following error message would be generated:

Router2# telnet 10.3.1.1

Trying 10.3.1.1Open

Password Required, but none set

[Connection to 10.3.1.1 closed by foreign host]

Router2#

The following set of commands would be used to configure the console password on a Cisco router, and so it is incorrect for this scenario.

Router(config)# line con 0

Router(config-line)# login

Router(config-line)# password john

The commands enable secret john and enable password john would be used to configure the enable secret password and the enable password for the router. However, they cannot be used to configure the Telnet password. Therefore, these options are incorrect.

Objective:

Infrastructure Management

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Configure and verify device management

References:

Licensed to Berend Post berend.post@it-university.nl

Question 49

Refer to the following sample output:

```
GigabitEthernet0/2 is up, line protocol is up
Internet address is 11.1.1.1/16
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN Flow CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is enabled, using route map PBR
Network address translation is disabled
BGP Policy Mapping is disabled
IP Multi-Processor Forwarding is enabled <======== MPF information
IP Input features, "PBR",
are not supported by MPF and are IGNORED
IP Output features, "NetFlow",
are not supported by MPF and are IGNORED
```

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

- ☐ show interfaces
- ☐ show interfaces summary
- ☒ show ip interface
- ☐ show interfaces serial

Explanation:

Explanation:

The show ip interface command will produce the displayed output. The show ip interface command is used to view the usability status of Internet Protocol (IP) interfaces. The complete syntax of this command is:

Licensed to Berend Post berend.post@it-university.nl

show ip interface [type number] [brief]

Following is a brief description of the parameters used in this command:

type: An optional parameter that refers to the type of interface.

number: An optional parameter that refers to the interface number.

brief: An optional parameter used to view a summarized display of the usability status information for every interface

The show interfaces command does not generate the displayed output. This command is used to view information regarding statistics for specific interfaces.

The show interfaces summary command does not generate the displayed output. This command provides a summarized view of all interfaces configured on a device.

The show interfaces serial command does not generate the displayed output. This command is used to view information for a serial interface.

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Licensed to Berend Post berend.post@it-university.nl

Question 50

You have executed the following commands on a switch:

Switch64(config)# interface range gigabitethernet2/0/1 -2
Switch64(config-if-range)# switchport mode access
Switch64(config-if-range)# switchport access vlan 10
Switch64(config-if-range)# channel-group 5 mode auto

In which of the following situations will Switch64 create an Etherchannel?

- ☒ If the other switch is set for desirable mode
- ☐ If the other switch is set for auto mode
- ☐ If the other switch is set for on mode
- ☐ If the other switch is set for passive mode

Explanation:

Explanation:

The Etherchannel will be created if the other end is set to desirable mode. The configuration shown in the example is using Port Aggregation protocol (PAGP). This protocol has two settings: desirable and auto. Two ends will negotiate and will only create an Etherchannel under two conditions: if one end is set to auto and the other end is set to desirable, or if both ends are set for desirable.

It will not form an Etherchannel if the other end is set to auto mode. When both ends are set to auto mode, an Etherchannel will not form.

It will not form an Etherchannel if the other end is set to on mode. On mode disables negotiation of any kind, which will prevent an Etherchannel from forming unless the other end is also set for on.

It will not form an Etherchannel if the other end is set to passive mode. Passive is a setting used in Link Aggregation Protocol (LACP). The two protocols are not compatible.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel

References:

Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE > Chapter: Configuring EtherChannels

Licensed to Berend Post berend.post@it-university.nl

Question 51

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

- ☒ encapsulation ppp
- ☐ encapsulation ip ppp
- ☐ ip encapsulation ppp
- ☐ encapsulation ppp-synch

Explanation:

Explanation:

PPP is a Layer 2 protocol encasulation type that supports both synchronous and asynchronous circuits and provides built-in security mechanaims. The encapsulation ppp interface configuration mode command is used to configure encapsulation for a PPP (Point to Point Protocol) serial link on a Cisco router. PPP encapsulation provides for router-to-router and host-to-network connections over both synchronous and asynchronous circuits. Serial links are configured to use Cisco High Level Data Link Control (HDLC) encapsulation, by default, on Cisco routers. The Cisco version of HDLC is incompatible with the industry standard version used on other router brands because it contains a type field that identifies the underlying network protocol being encapsulated by HDLC. This is a beneficial feature of Cisco HDLC but makes it incompatible with other router brands.

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

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

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Router1(config)#interface Serial0

Router1(config-if)#encapsulation ppp

Router1(config-if)#ppp authentication pap

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

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

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

encapsulation ppp

encapsulation hdlc

encapsulation frame relay

All other options are invalid commands.

Objective:

WAN Technologies

Sub-Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

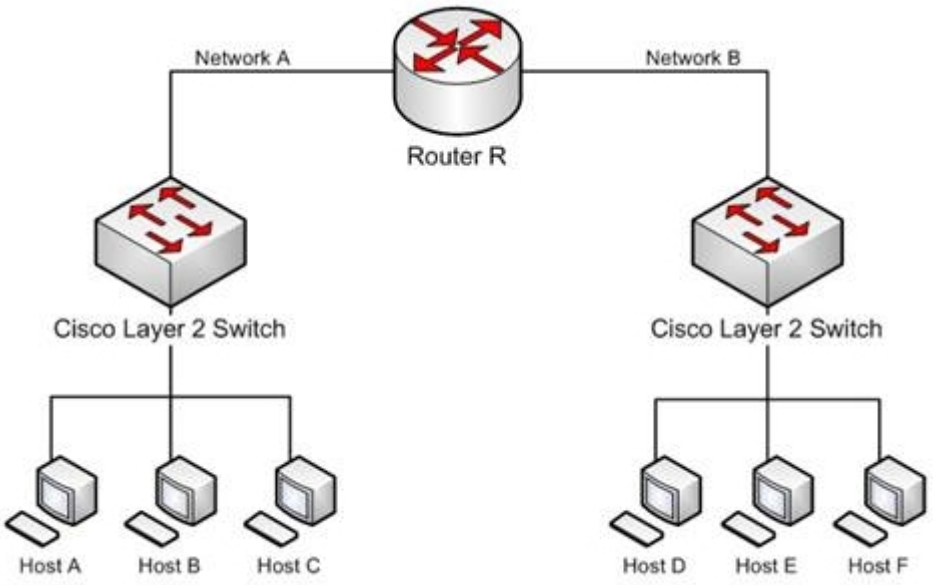
References:

Internetworking Technology Handbook > WAN Technologies > Point-to-Point Protocol

Licensed to Berend Post berend.post@it-university.nl

Question 52

Refer to the network diagram in the exhibit. Host A is configured with an incorrect default gateway. All other computers and the Router are known to be configured correctly (Click the Exhibit(s) button.)



Which of the following statements is TRUE?

- ☐ Host C on Network A cannot communicate with Host A on Network A.
- ☒ Host A on Network A can communicate with all other hosts on Network A.
- ☒ Host A on Network A can communicate with Router R.
- ☐ Host C on Network A cannot communicate with Router R.
- ☐ Host D on Network B cannot communicate with Host B on Network A.

Explanation:

Explanation:

Host A on Network A can communicate with all other hosts on Network A and with Router R. To communicate with local hosts and the interface of Router R (which are all in the same subnet) only a correct IP address is reqired. If the default gateway of Host A is incorrect, then it will not be able to communicate with any host on the other side of the router, which includes Network B in the diagram. Packets from hosts on Network B will reach Host A on Network A without any problem, because they possess the correct address of the default gateway or router, but Host A will send the packet to a dead end because Host A has an incorrect default gateway. On the other hand, Host A does not require a default gateway to communicate with other hosts on same network.

Host C on Network A WILL be able to communicate with Host A on Network A , even though Host A has an incorrect default gateway because Host A and C are in the same subnet, which requires no use of the of the gateway or router..

Licensed to Berend Post berend.post@it-university.nl

Host C on Network A WILL be able to communicate with Router R because Host C has the correct default gateway address which is the address of Router R.

Host D on Network B WILL be able to communicate with Host B on Network A because both hosts have a correct default gateway address.

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

Cisco > Internetworking Technology Handbook > Internetworking Basics > Routing Basicshttp://www.microsoft.com/technet/community/columns/cableguy/cg0903.mspx

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

Question 53

What is the significance of the following BECN packet statistics?

```
Router# show frame-relay pvc 16

PVC Statistics for interface serial0 (Frame Relay DTE)

DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0
input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 0 in FECN pkts 0
in BECN pkts 100 out FECN pkts 0 out BECN pkts 0
<<output omitted>>
```

- ☒ The router is experiencing congestion in sending frames.
- ☐ The router is experiencing congestion in receiving frames.
- ☐ The Frame Relay mapping table is missing an entry.
- ☐ The Frame Relay mapping table is corrupt.

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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

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

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

Objective:

WAN Technologies

Sub-Objective:

Describe basic QoS concepts

References:

Cisco > Home > Support > Technology Support > WAN > Frame Relay > Design > Design TechNotes > show Commands for Frame Relay Traffic Shaping

Licensed to Berend Post berend.post@it-university.nl

Question 54

You have been asked to examine the following output to identify any security problems with the router. Its configuration is shown:

```
Current configuration:
!
version 11.2
!
hostname cisco
!
enable secret 5 $1$mERr$7sOd0mgRuXYhHwfWsV4QZ/
!
banner login ^C Welcome to Router 5 Authorized users only ^C
!
interface Ethernet0
ip address 10.1.1.1 255.0.0.0
!
interface Serial0
ip address 20.2.2.2 255.0.0.0
!
router rip
network 10.0.0.0
network 20.0.0.0
!
ip route 0.0.0.0 0.0.0.0 20.2.2.3
!
line vty 0 4
password Cisc0$ell$
no login
!
end
```

What problems exist? (Choose all that apply.)

- ☐ unencrypted privileged mode password
- ☒ inappropriate wording in the banner message
- ☐ weak password on the VTY line
- ☒ Telnet users will not be prompted for a password

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > Part 1: Cisco IOS User Interfaces Commands > Connection, Menu, and System Banner Commands > banner login

Question 55

You have executed the following commands on switch55:

```
switchA(config)# dot1x system-auth-control
switchA(config)# aaa new-model
switchA(config)# radius-server host 192.168.105.67 key firstKey111
switchA(config)# aaa authentication dot1x default group radius
switchA(config)# interface range Fa 0/1 - 11
switchA(config-if)# switchport mode access
switchA(config-if)# dot1x port-control auto
```

What is the result of executing the given commands? (Choose two.)

- ☒ Only the listed RADIUS server is used for authentication
- ☐ 802.1X authentication is enabled on the Fa0/1 interface only
- ☒ The key for the RADIUS server is firstKey111
- ☐ AAA is not enabled on the switch

Explanation:

Explanation:

As a result of executing these commands, the default list is used for the RADIUS server for authentication, and the key for the RADIUS server is firstKey111.

A RADIUS server combines the authentication and authorization processes. Before you configure the RADIUS server, you should enable AAA by using the aaa new-model command in global configuration mode. Then, you can specify the location of the RADIUS server and the key using the radius-server host command. In this case, the RADIUS server is located at the IP address 192.168.105.67 and requires the key firstKey111 as the encryption key. This key must be mutually agreed upon by the server and the clients.

Licensed to Berend Post berend.post@it-university.nl

The aaa authentication dot1x default group radius command creates a method list for 802.1X authentication. The default group radius keywords specify that the default method will be to use all listed RADIUS servers to authenticate clients. Since only one is listed, it will be the only one used.

It is incorrect to state that 802.1X authentication is enabled only on the Fa0/1 interface. The interface range Fa 0/1 - 11 and the dot1x port-control auto commands specify that 802.1X authentication is enabled on the interfaces Fa0/1 to Fa0/11.

It is incorrect to state that AAA is not enabled on the switch. The aaa new-model command enables AAA globally on the switch.

Objective:

Infrastructure Security

Sub-Objective:

Describe device security using AAA with TACACS+ and RADIUS

References:

Cisco > Support > Cisco IOS Security Command Reference: Commands A to C > aaa new-model

Cisco > Support > Cisco IOS Security Command Reference: Commands D to L > dot1x port-control

Cisco > Support > Cisco IOS Security Command Reference: Commands M to R > radius-server host

Licensed to Berend Post berend.post@it-university.nl

Question 56

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?

- ☐ The default gateway address is incorrect
- ☒ The IP address of the device is incorrect
- ☐ There is no DNS server configured
- ☐ IP routing is not enabled

Explanation:

Explanation:

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

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

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

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Services

Sub-Objective:

Describe DNS lookup operation

References:

PChuck's Network > Microsoft Windows Networking, Security, and Support > Reading IPConfig and Diagnosing Network Problems

Question 57

You have two routers in your OSPF area 0. Router 1 is connected to Router 2 via its Serial 1 interface, and to your ISP via the Serial 0 interface. Router 1 is an ASBR.

After your assistant configures a default route on Router 1, you discover that whenever either router receives packets destined for networks that are not in the routing tables, it causes traffic loops between the two routers.

To troubleshoot, you execute the show run command on Router 1. Part of the output is shown below:

<output omitted>
IP route 0.0.0.0 0.0.0.0 serial 1
Router ospf 1
Network 192.168.5.0 0.0.0.255 area 0
Default-information originate

Which command or set of commands should you execute on Router 1 to stop the looping traffic while maintaining Router 2's ability to send traffic to the Internet?

- ☐ Execute the no default-information originate command.
- ☒ Execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command and then execute the ip route 0.0.0.0 0.0.0.0 serial 0 command.
- ☐ Execute the default-information originate always command.
- ☐ Execute the no network 192.168.5.0 area 0 command and then execute the network 192.168.5.0 255.255.255.0 area 0 command.

Explanation:

Explanation:

You should execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command followed by the ip route 0.0.0.0 0.0.0.0 serial 0 command. The original configuration command was executed on the wrong interface on Router 1 by your assistant. It should be executed on Serial 0, which is the connection to the ISP. The show run command indicates that with the current configuration, if Router 2 receives a packet not in its table, it sends it to Router 1, and then Router 1 sends it back out on Serial 1. This redirects

 Licensed to Berend Post berend.post@it-university.nl

the packet back to Router 2, and the loop begins. By changing the configuration to Serial 0, Router 1 will start forwarding all traffic not in the routing table to the ISP.

You should not execute the no default-information originate command. This command instructs Router 1 to NOT inject the default route into area 0, which is the desired behavior. Running this command would stop the loop, but would leave Router2 with no default route to send packets to the Internet.

You should not execute the default-information originate always command. The addition of the always parameter instructs Router 1 to inject a default route into area 0, even if one does not exist on Router 1. This is unnecessary, since Router 1 does have a default route configured, and will not change the existing looping behavior.

You should not execute the no network 192.168.5.0 area 0 command followed by the network 192.168.5.0 255.255.255.0 area 0 command. There is nothing wrong with the original network command. Also, the network 192.168.5.0 255.255.255.0 area 0 command uses an incorrect mask type. The mask must be in the wildcard format. Moreover, since it is incorrect, this will have the effect of disabling OSPF on the network connecting the two routers.

Objective:

Routing Fundamentals

Sub-Objective:

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

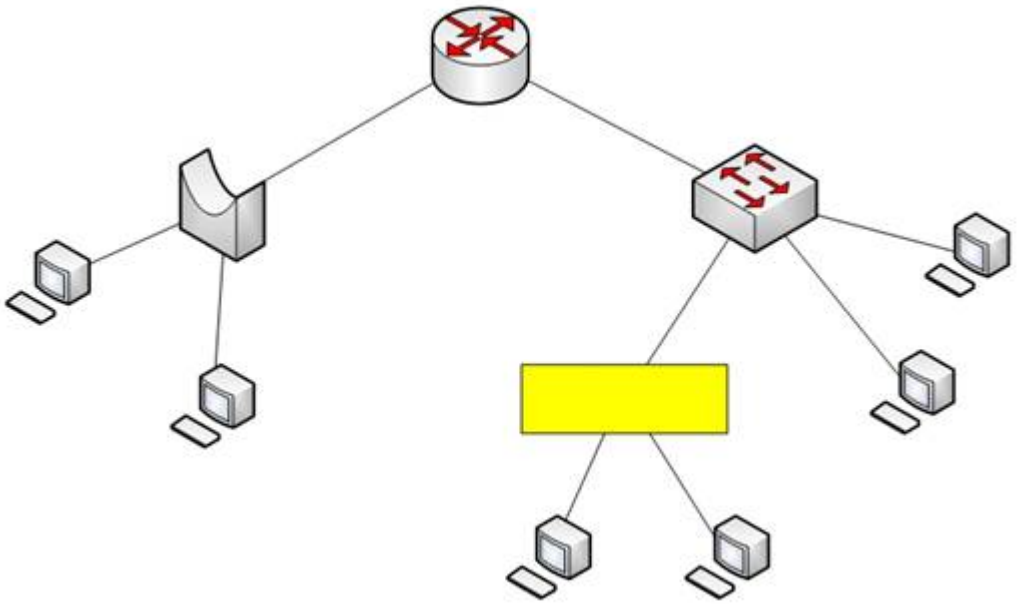
References:

Cisco > Home > Support > Technology Support > IP > IP Routing > Configure > Configurations Examples and Technotes > How OSPF Injects a Default Route into a Normal Area

Licensed to Berend Post berend.post@it-university.nl

Question 58

Assume that all ports on Layer 2 devices are in the same Virtual LAN (VLAN). View the given network topology. (Click the Exhibit(s) button.)



Which network device should be placed at the highlighted box to produce a total of two broadcast domains and seven collision domains in the network?

- ☒ Hub
- ☐ Bridge
- ☐ Switch
- ☐ Router

Explanation:

Explanation:

A hub should be placed at the highlighted box to produce a total of two broadcast domains and seven collision domains in the network. Network devices segment collision domains and broadcast domains in the following manner:

Hub: A Layer 1 device with all ports in same collision domain and broadcast domain.

Bridge/Switch: Layer 2 devices on which all ports are in different collision domains, but in the same broadcast domain (assuming that all ports are in the same VLAN or no VLAN is configured).

Routers: A Layer 3 device on which every port is a separate collision as well as broadcast domain.

The bridge shown in the graphic has three ports populated by active links, resulting in three collision domains. The switch shown in the exhibit has four ports populated with the links, resulting in four collision domains. Together these two devices create seven collision domains.

Licensed to Berend Post berend.post@it-university.nl

Because the scenario requires that there be no more than seven collision domains, the device in the highlighted box must not create any further collision domains. A hub is a device that has all its ports in the same collision domain and will not create any further collision domains in the topology.

A bridge or switch cannot be the correct option because these will also add collision domains.

In the exhibit, the router has two ports with active links, which will result into two broadcast domains. Because the scenario states there are no more than two broadcast domains, the device in the highlighted box must not be a router. Routers are used to segment broadcast domains.

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

References:

Question 59

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

- ☒ ip classless
- ☐ no ip classless
- ☐ auto-summary
- ☐ no auto-summary

Explanation:

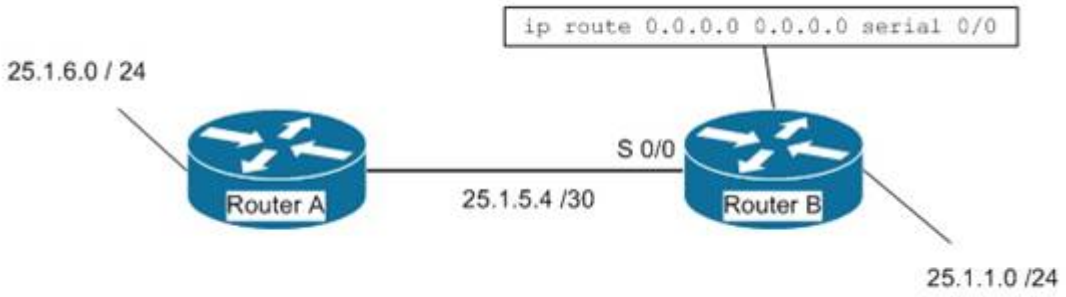
Explanation:

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

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

Licensed to Berend Post berend.post@it-university.nl

statically configured default route to forward traffic to an unknown subnet of that network (in this case 25.1.6.0/24). In the scenario described in the diagram, Router B will drop the packet. However, if the ip classless command has been executed, it will use the default route and send the traffic to Router A.



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

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

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

Licensed to Berend Post berend.post@it-university.nl

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

Question 60

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?

- ☐ Source IP address
- ☒ Destination MAC address
- ☐ Source port number
- ☐ Destination IP address

Explanation:

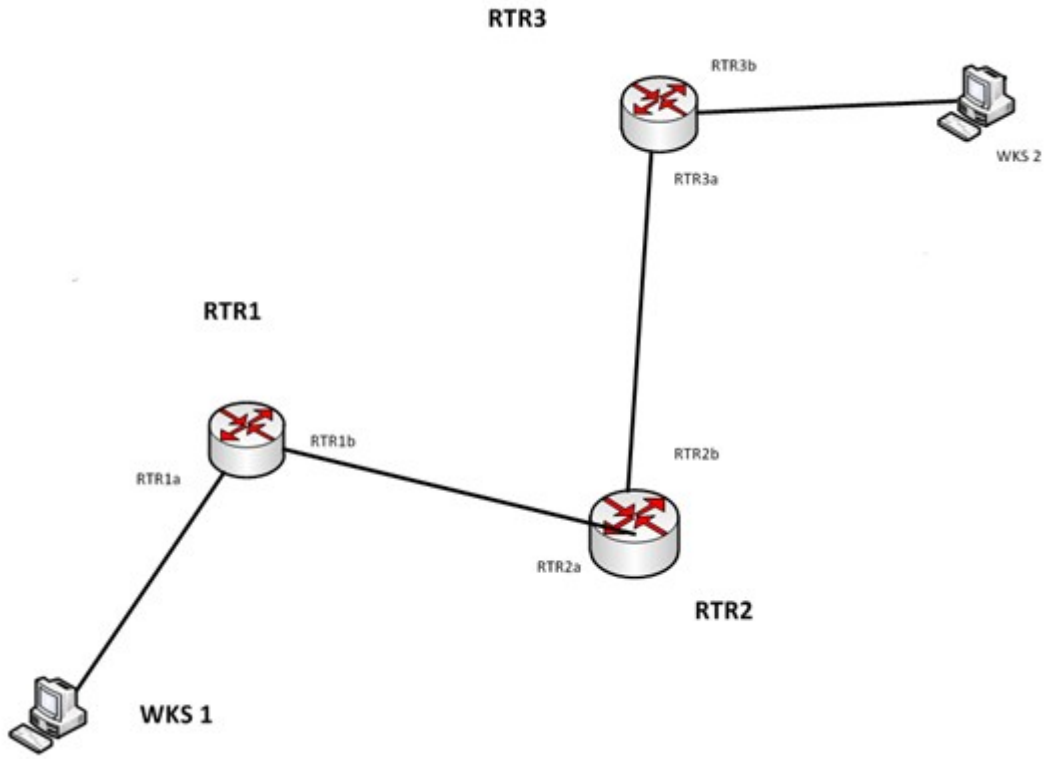
Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl



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

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

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

Handoff	Packet (IP) destination address	Frame (MAC) Destination Address
WKS1 to RTR1a	27.3.5.10	b-b-b-b-b-b
RTR1b to RTR2a	27.3.5.10	d-d-d-d-d-d
RTR2b to RTR3a	27.3.5.10	f-f-f-f-f-f
RTR3b to WKS2	27.3.5.10	h-h-h-h-h-h

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

Objective:

Licensed to Berend Post berend.post@it-university.nl

LAN Switching Fundamentals

Sub-Objective:

Interpret Ethernet frame format

References:

MAC address changes for every new network

Question 61

Which Network Address Translation (NAT) term is used for the IP address that is assigned to a host on the inside network?

- ☒ Inside local address
- ☐ Inside global address
- ☐ Outside local address
- ☐ Outside global address

Explanation:

Explanation:

An inside local address is the NAT term that is used to describe the IP address assigned to a host on the inside network. It is usually a private IP address.

An inside global address is the registered IP address assigned by the ISP, which represents one or more inside local IP addresses externally.

An outside local address is the IP address of an external host as it appears to the internal network.

An outside global address is the IP address assigned to a host on the external network by the host owner. The address is allocated from a globally routable address space.

NAT enables companies to use one IP addressing scheme within their network but translate those IP addresses for external communication. Static NAT assigns a permanent one-to-one mapping of local addresses to global addresses. Dynamic NAT assigns address mappings by using a pool of available addresses. NAT overloading or Port Address Translation (PAT) reduces the number of global addresses required by allowing multiple local hosts to share a global address.

Objective:

Infrastructure Services

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure, verify, and troubleshoot inside source NAT

References:

Cisco > Support > Technology Support > IP > IP Addressing Services > Design > Design TechNotes > NAT: Local and Global Definitions

Cisco > Articles > Network Technology > General Networking > Network Address Translation

Question 62

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

- ☐ inter-VLAN routing
- ☐ encryption of network packets
- ☒ frame identification over trunk links
- ☐ frame identification over access links

Explanation:

Explanation:

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

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

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

Licensed to Berend Post berend.post@it-university.nl

router# show interfaces fastEthernet 0/0.1

FastEthernet0/0.1 is up, line protocol is up

Hardware is AmdFE, address is 0003.e36f.41e0 (bia 0003.e36f.41e0)

Internet address is 10.10.10.1/24

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ISL Virtual LAN, Color 1.

ARP type: ARPA, ARP Timeout 04:00:00

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Cisco > Cisco IOS LAN Switching Configuration Guide, Release 12.4 > Part 1: Virtual LANs > Routing Between VLANs Overview

Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format > Document ID: 17056

Question 63

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

- ☐ 32
- ☒ 62
- ☐ 128
- ☐ 256

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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

The formula to calculate the available number of hosts is:

2n - 2 = x

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

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

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

Number of hosts = 26 - 2

Number of hosts = 64 - 2 = 62

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

11111111.11111111.1111111.11000000

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

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

Licensed to Berend Post berend.post@it-university.nl

Network address: 192.168.12.0

Subnet Mask in decimal: 255.255.255.192

Subnet Mask in binary: 11111111.11111111.11111111.11000000

Hosts: 64 - 2 = 62

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

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Cisco > Design Tech Notes > IP Routing > IP Addressing and Subnetting for New Users > Understanding IP Addresses > Document ID: 13788

Nooning, Thomas. "TechRepublic Tutorial: Subnetting a TCP/IP Network." TechRepublic, 20 May 2003.

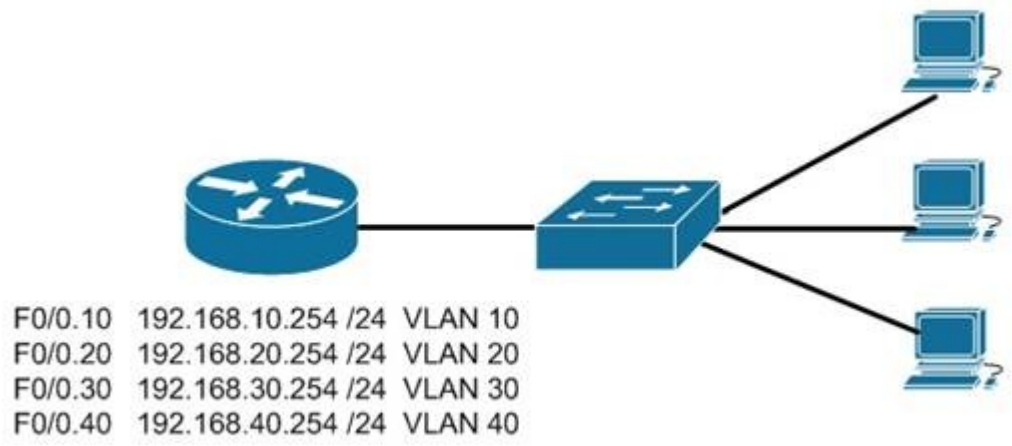
Licensed to Berend Post berend.post@it-university.nl

Question 64

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?

- ☐ Connect the new computer to Fa0/1
- ☐ Connect the new computer to Fa0/14
- ☒ Connect the new computer to Fa0/5
- ☐ Configure a dynamic routing protocol on the router interface

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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

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

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

1 default active Fa0/1, Fa0/2, Fa0/3,

Fa0/7, Fa0/8, Fa0/9,

Fa0/14, Fa0/16, Fa0/23,

Fa0/19, Fa0/20, Fa0/23

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Cisco > Support > Cisco IOS LAN Switching Command Reference > show vlan

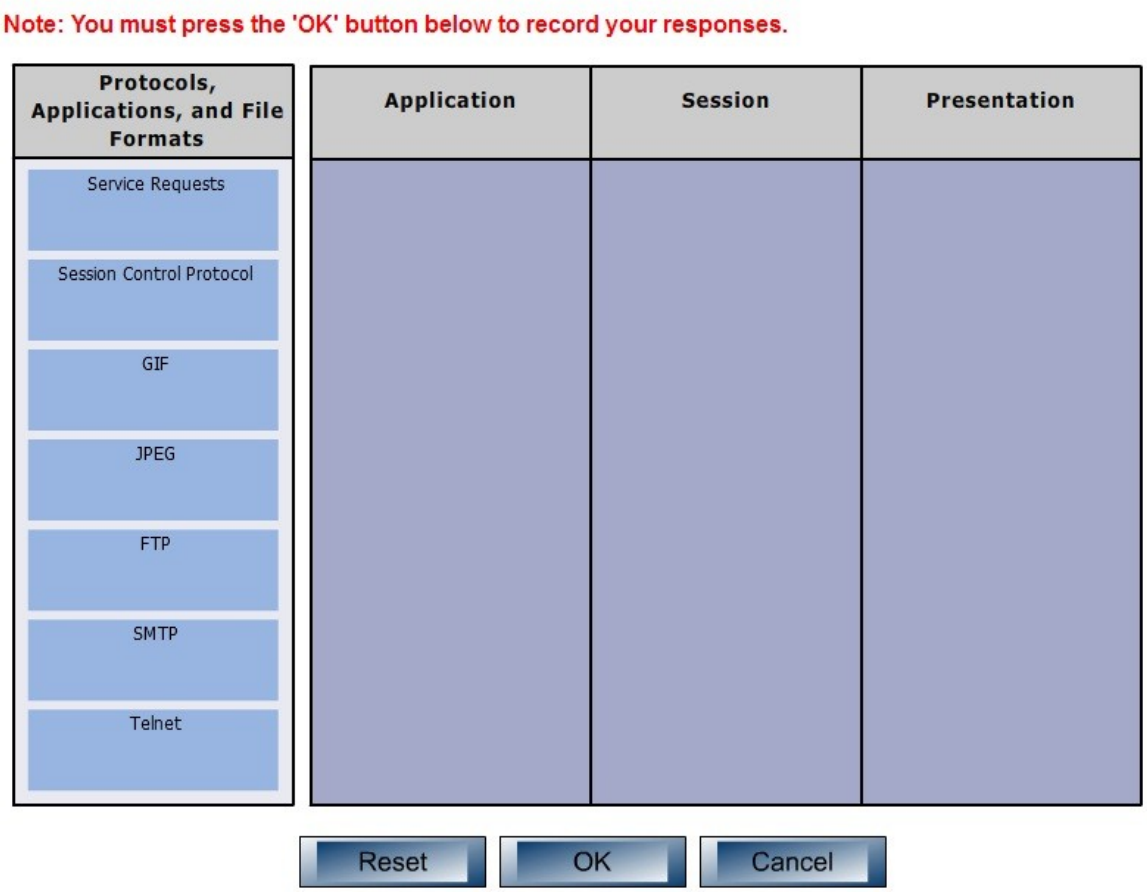
Cisco Networking Essentials 2nd Edition, by Troy McMillan (ISBN 1119092159). Sybex, 2015. Chapter 15: Configuring Inter-VLAN Routing

Licensed to Berend Post berend.post@it-university.nl

Question 65

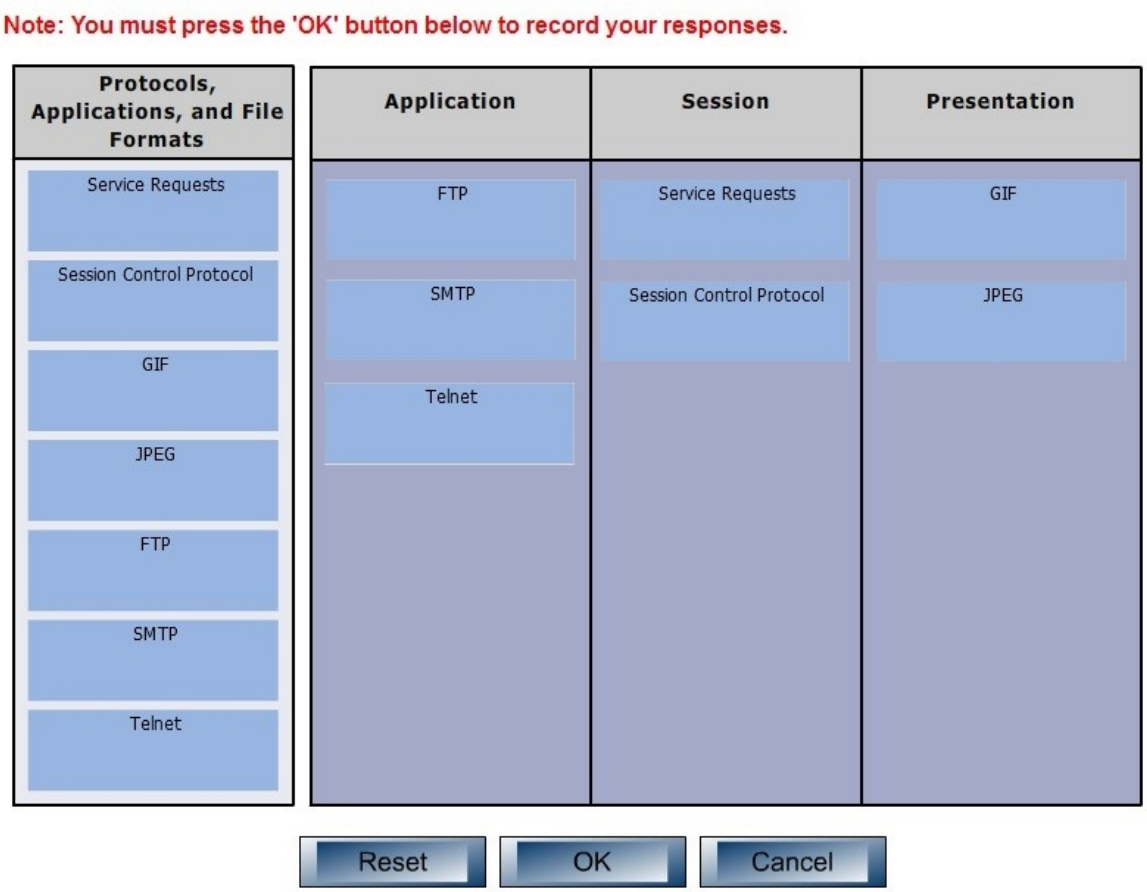
DRAG DROP

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



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

Explanation:

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

FTP: Used to transfer data between hosts through the Internet or a network.

SMTP: SMTP is a Transmission Control Protocol (TCP)/Internet Protocol (IP) protocol which is used to send and receive e-mail messages.

Telnet: Used to allow remote logins.

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

Service requests: Service requests and service responses which take place between different applications are handled by the session layer.

Session Control Protocol (SCP): Allows a host to have multiple conversations with another host using the same TCP connection.

Licensed to Berend Post berend.post@it-university.nl

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

Graphics Interchange Format (GIF)

Joint Photographic Experts Group (JPEG)

Tagged Image File Format (TIFF)

Other layers in the OSI model include:

Transport: Responsible for error free and sequential delivery of data. This layer is used to manage data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Physical: Consists of hardware for sending and receiving data on a carrier. The protocols which work at the Physical layer include Fast Ethernet, RS232, and Asynchronous Transfer Mode (ATM).

Network: Used to define the network address or the Internet Protocol (IP) address which is then used by the routers to forward make forwarding decisions.

Data Link: Ensures reliable transmission of data across a network on the basis of Layer 2 addresses such as MAC addresses (Ethernet) or DLCIs (Frame Relay).

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast TCP and UDP protocols

References:

Cisco Documentation > Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems

Licensed to Berend Post berend.post@it-university.nl

Question 66

What switch security configuration requires AAA to be configured on the switch?

- ☐ VACL
- ☒ 802.1x
- ☐ Private VLAN
- ☐ port security

Explanation:

Explanation:

802.1x requires AAA to be configured on the switch. 802.1x uses AAA authentication to control access to the port.

The overall steps required to configure a switch for 802.1x are:

Enable AAA on the switch.

Define the external RADIUS server(s) and the key to be used for encryption.

Define the authentication method.

Enable 802.1x on the switch.

Configure each switch port that will use 802.1x.

Optionally allow multiple hosts on the switch port.

Objective:

Infrastructure Security

Sub-Objective:

Describe device security using AAA with TACACS+ and RADIUS

References:

Consolidated Platform Configuration Guide, Cisco IOS XE Release 3E (Cisco 5700 Series WLC) - Configuring IEEE 802.1x Port-Based Authentication (PDF)

Licensed to Berend Post berend.post@it-university.nl

Question 67

Which of the following commands could you use to verify the type of serial cable you are connected to (DCE or DTE)?

- ☐ show interfaces
- ☒ show controllers
- ☐ show ip interface
- ☐ show interface dce
- ☐ show interface switchport

Explanation:

Explanation:

The show controllers command provides hardware-related information used to troubleshoot and diagnose issues with Cisco router interfaces. The output of the command is as follows:

routerA# show controllers serial 0

HD unit 1, idb = 0x1C44E8, driver structure at 0x1CBAC8

buffer size 1524 HD unit 1

V.35 DTE cable, clock rate 64000

The preceding output indicates that a V.35 DTE cable is currently connected to interface Serial 0, and that a clock rate of 64000 bps has been detected from the DCE (the other side of the serial link). When the other end is a CSU/DSU, as is usually the case, the clock rate is provided by the CSU/DSU. The clocks stopped portion of the following output would indicate that a clock rate has not been detected from the DCE:

routerA# show controllers serial 0

HD unit 1, idb = 0x1C44E8, driver structure at 0x1CBAC8

buffer size 1524 HD unit 1

V.35 DTE cable, clocks stopped

This condition would be rectified by configuring a clock rate on the DCE router.

The show interfaces, show ip interface, and show interface switchport commands do not display any hardware-related information, such as connected cable types.

The show interface dce command is incorrect because this is not a valid Cisco IOS command.

Licensed to Berend Post berend.post@it-university.nl

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Question 68

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

- ☐ ipv6 address 5000::2222:1/64
- ☒ ipv6 address autoconfig
- ☐ ipv6 address 2001:db8:2222:7272::72/64 link-local
- ☐ ipv6 enable

Explanation:

Explanation:

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

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

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

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

Objective:

 Licensed to Berend Post berend.post@it-university.nl

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv6 addressing

References:

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

Cisco > Support > Cisco IOS IPv6 Command Reference > ipv6 address

Question 69

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

- ☒ The decimal values of the first octet can range from 192 to 223
- ☐ The decimal values of the first octet can range from 1 to 126
- ☐ The first octet represents the entire network portion of the address
- ☒ The first three octets represent the entire network portion of the address
- ☐ The value of the first binary place in the first octet must be 0
- ☒ The value of the first two binary places in the first octet must be 11

Explanation:

Explanation:

A class C IP addresses will have the following characteristics:

The decimal values of the first octet can range from 192 to 223

The first three octets represent the entire network portion of the address

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

Class B IP addresses will have the following characteristics:

The decimal values of the first octet can range from 128 to 191

The first two octets represent the entire network portion of the address

The value of the first two binary place in the first octet must be 10

Class A IP addresses will have the following characteristics:

The decimal values of the first octet can range from 1 to 126

The first octet represents the entire network portion of the address

The value of the first binary place in the first octet must be 0

 Licensed to Berend Post berend.post@it-university.nl

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast IPv4 address types

References:

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

Question 70

Which of the following excerpts from the output of the show ip eigrp topology command include EIGRP learned routes or pairs of routes that will be included in the routing table? (For excerpts that include multiple routes, do not include the entry unless BOTH routes will be included in the routing table.)

- ☐ P 172.16.16.0/24, 1 successors, FD is 284244
- ☐ via 172.16.250.2 (284244/17669856), Serial0/0
- ☐ via 172.16.251.2 (12738176/27819002), Serial0/1
- ☐ P 172.16.250.0/24, 1 successors, FD is 2248564
- ☐ via Connected, Serial0/0
- ☒ P 172.16.10.0/24 2 successors, FD is 284244
- ☒ via 172.16.50.1 (284244/17669856), Serial1/0
- ☒ via 172.16.60.1 (284244/17669856), Serial1/1
- ☐ P 172.16.60.0/24, 1 successors, FD is 2248564
- ☐ via Connected, Serial1/1

Explanation:

Explanation:

The following excerpt indicates two successor routes, and they will both be included:

P 172.16.10.0/24 2 successors, FD is 284244

via 172.16.50.1 (284244/17669856), Serial1/0

via 172.16.60.1 (284244/17669856), Serial1/1

Both of these routes will be included because they have identical metrics (284244/17669856). Only the EIGRP successor routes will appear in the routing table, as these are considered the best-path routes to each remote network.

 Licensed to Berend Post berend.post@it-university.nl

The route for 172.16.16.0/24 via 172.16.251.2 (12738176/27819002) will not be included because only successor routes are included, and this route is a feasible successor. Feasible successor routes are routes that are used only as a backup if the successor route(s) becomes unavailable. If you examine the output of each option, it will indicate how many successor routes are in the entry. The entry shows that there is only one successor to this route:

P 172.16.16.0/24, 1 successors, FD is 284244

via 172.16.250.2 (284244/17669856), Serial0/0

via 172.16.251.2 (12738176/27819002), Serial0/1

The first listed is the successor and the second is the feasible successor. The first has the best or lowest metric (284244/17669856), which is the criterion used for selection.

These entries indicate successor routes, but they also indicate they are via Connected, which means they are networks directly connected to the router.

P 172.16.250.0/24, 1 successors, FD is 2248564

via Connected, Serial0/0

and

P 172.16.60.0/24, 1 successors, FD is 2248564

via Connected, Serial1/1

Therefore, they are not EIGRP learned routes.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Cisco IOS IP Routing Protocols Command Reference > EIGRP Commands: M through V > show ip eigrp topology

Question 71

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

- ☒ A LAN is confined to one building or campus.
- ☐ A LAN can cover great distances.
- ☒ A LAN provides fast data transmission.
- ☒ A LAN is easily expandable.
- ☐ LANs require the use of a router to communicate between local hosts.

Explanation:

Explanation:

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

The following are some characteristics of LANs:

LANs are generally confined to a building, a group of buildings, or a campus.

Every computer in the LAN can communicate with every other computer on the network.

A LAN is easy to set up, as physical connectivity can be easily established.

The cost of the transmission medium used is low, as a LAN generally uses CAT5, CAT5e, or CAT6 cables for data transmission.

A LAN provides fast data transmission rates.

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

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

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast network topologies

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco Documentation > Internetworking Technology Handbook > Introduction to LAN Protocols

Question 72

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

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

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

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

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

Explanation:

Explanation:

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

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

Question 73

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

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

C 192.8.1.1/32 directly connected to loopback 0

- ☐ This is a default route
- ☒ This is an EIGRP route
- ☐ This is static route
- ☐ This is a directly connected route

Explanation:

Explanation:

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

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

 Licensed to Berend Post berend.post@it-university.nl

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

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Cisco > Support > Cisco IOS IP Routing: Protocol-Independent Command Reference > show ip route

Question 74

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?

- ☐ tracert
- ☒ traceroute
- ☐ extended ping
- ☐ ping

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

```
Type escape sequence to abort.
Tracing the route to 33.0.0.4

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

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

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > traceroute

Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730 > The Extended ping Command

Cisco Documentation > Internetwork Troubleshooting Handbook > Troubleshooting TCP/IP

Licensed to Berend Post berend.post@it-university.nl

Question 75

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

Which deployment model should be implemented to accomplish the task?

- ☐ IPv6 over IPv4 tunnels
- ☐ IPv6 over dedicated Wide Area Network (WAN) links
- ☒ Dual-Stack Backbones
- ☐ Protocol translation

Explanation:

Explanation:

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

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

IPv6 over IPv4 tunnels: IPv6 traffic is encapsulated into IPv4 packets. Then these packets are transferred over an IPv4 WAN. This model eliminates the need to create separate circuits to connect to the IPv6 networks. This model increases protocol overhead because of the IPv6 headers and requires one end to be capable of both protocols

Protocol translation: A translation method of allowing an IPv6 host to communicate with an IPv4 host. This is accomplished with the help of Network Address Translation - Protocol Translation (NAT-PT) used to configure translation between IPv6 and IPv4 hosts. NAT-PT allows communication between IPv6 hosts and applications, and native IPv4 hosts and applications.

IPv6 over dedicated WAN links: A new deployment of IPv6 is created. In this model, IPv6 hierarchy, addressing, and protocols are used by all nodes. However, this model involves cost for creating IPv6 WAN circuits. This solution is not designed for LAN translation but rather translation over WAN links.

Dual-Stack Backbones: A hybrid model in which backbone routers have dual-stack functionality, which enables them to route both IPv4 and IPv6 packets. It is suitable for an enterprise that uses both IPv4 and IPv6 applications. Running IPv6 and IPv4 together in a network is known as dual-stack routing.

Objective:

Network Fundamentals

Sub-Objective:

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

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Dual Stack Network

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

Question 76

You have a Telnet session established with a switch from a router. You would like to maintain that connection while you return to the session with the router, and then easily return to the switch session after connecting to the router.

What command should you use?

- ☒ <Ctrl-Shift-6>x
- ☐ resume
- ☐ suspend
- ☐ <Ctrl-Alt-6>shift

Explanation:

Explanation:

After typing the Ctrl-Shift-6 sequence, you can tap the x key and return to the previous session, which in this case was the session with the router. Below is the full sequence of commands described in this item:

Router1#telnet 192.168.3.3

Tying 192.168.3.3..Open

User Access Verification

Password:

Switch2><Ctrl-Shift-6>x

Router1#

When you desired to return to the session with the switch, you would use the resume command as shown below:

Router1#resume

Switch>

Neither the suspend nor the <Ctrl-Alt-6>shift commands are valid commands.

 Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

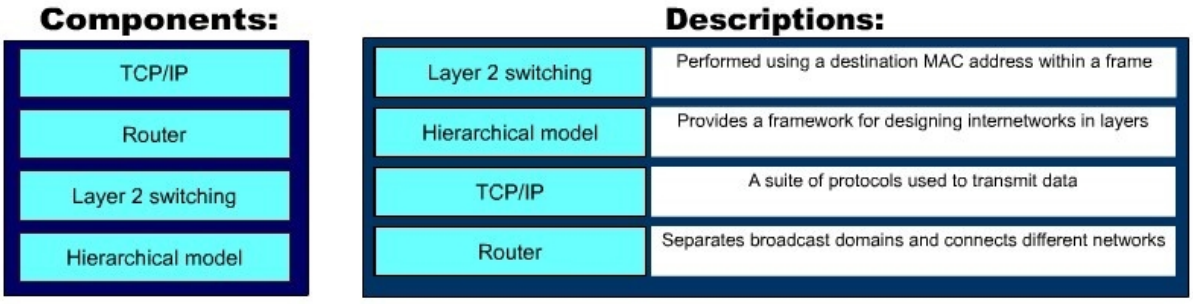
Establishing Telnet Sessions>Suspending and Terminating Telnet Sessions

Question 77

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



Solution:



Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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 internetworks 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:

Cisco wiki > Main Page > Internet Protocols

Cisco wiki > Internetwork Design Guide -- Designing Switched LAN Internetworks > General Network Design Principles > 5.6.1 Figure: Hierarchical network design model

Question 78

Which device creates broadcast domains and enables communication across separate broadcast domains?

- ☒ router
- ☐ switch
- ☐ hub
- ☐ access points

Explanation:

Explanation:

A router allows communication across separate broadcast domains. A broadcast domain is group of hosts and network devices in which a broadcast frame sent by one host can be received by all of the other hosts in the broadcast domain. A router determines the path to other destination networks, and forwards data packets to the next hop along this path. A router operates at Layer 3 of the Open System Interconnect (OSI) layered communication model and uses an Internet Protocol (IP) address hierarchy to identify and route data through source and destination devices.

Licensed to Berend Post berend.post@it-university.nl

A switch does not allow communication across separate broadcast domains. A switch creates collision domains and enables communications across different collision domains. A collision domain is a logical group of hosts and network devices where packets can potentially collide with one another, causing a communications disruption. Switches forward broadcasts so they do not form a separate broadcast domain unless Virtual LANs (VLANs) are created.

A hub does not allow communication across separate broadcast domains. A hub transmits frames, which means that they neither form separate collision or broadcast domains nor allow communication across these domains. Hubs are multiport devices that allow consolidation of various LAN segments and amplify signals that pass through them. Hubs operate at OSI Layer 1.

An access point does not allow communication across separate broadcast domains. Access points (APs) are OSI Layer 2 wireless hubs that allow client hosts to connect to the backbone network wirelessly.

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

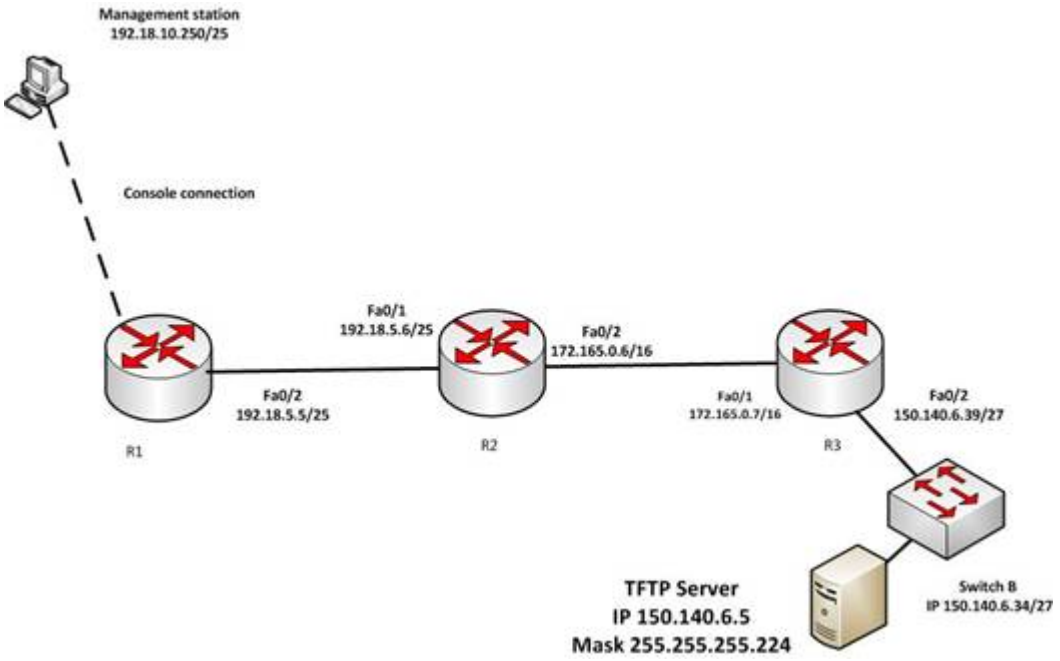
References:

Cisco > Home > Internetworking Technology Handbook > Internetworking Basics> Bridging and Switching Basics

Licensed to Berend Post berend.post@it-university.nl

Question 79

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



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

- ☐ The IP address of the management station is incorrect
- ☒ The IP address of the TFTP server is incorrect
- ☐ The interfaces between R1and R2 are not in the same subnet
- ☐ The IP address of Switch B is incorrect

Explanation:

Explanation:

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

150.140.0.0

150.140.0.32

150.140.0.64

and so on, incrementing in intervals of 32 in the last octet until it reaches the 150.140.6.0 subnet.

150.140.6.0

150.140.6.32

Licensed to Berend Post berend.post@it-university.nl

150.140.6.64

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

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

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

192.18.5.0

192.168.5.128

Both router interfaces in question are in the 192.18.5.0 subnet.

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

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 80

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

```
Access1#show spanning-tree vlan 10

VLAN0010

Spanning tree enabled protocol rstp
Root ID Priority 24586
Address 0015.63f6.b700
Cost 19
Port 107 (FastEthernet3/0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 000f.f794.3d00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa3/0/1 Root FWD 19 128.107 P2p
Fa3/0/2 Altn BLK 19 128.108 P2p
--------------------------------------------------------------------------
```

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

Explanation:

Explanation:

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Cisco IOS Bridging Command Reference > show spanning-tree

Question 81

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

- ☐ client
- ☐ server
- ☒ virtual
- ☐ transparent

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

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

Question 82

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

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

Explanation:

Explanation:

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

The following statements are true of public IP addressing:

These addresses are publicly registered with the Internet Assigned Numbers Authority (IANA)

Through a public IP address, you can access another Internet computer, such as a Web server.

Other people on the Internet can obtain information about or access to your computer via a public IP address.

Public IP addresses are visible to the public.

 Licensed to Berend Post berend.post@it-university.nl

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Describe the need for private IPv4 addressing

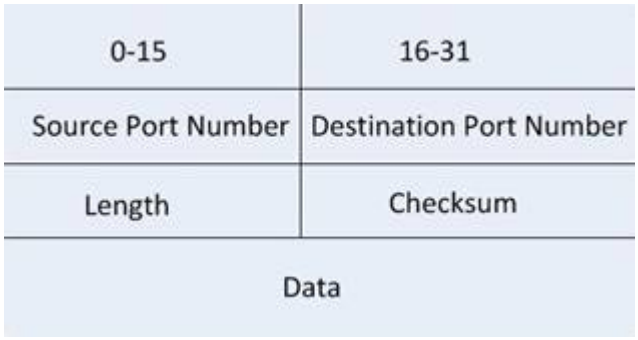
References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 83

What data structure is pictured in the graphic?



- ☐ TCP segment
- ☒ UDP datagram
- ☐ IP header
- ☐ Http header

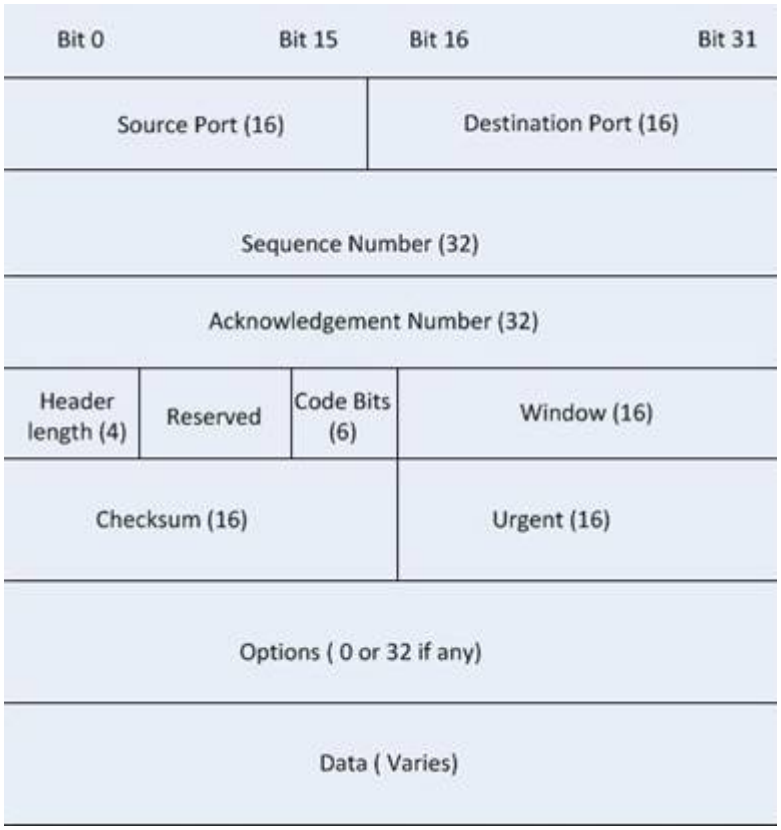
Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl



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

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

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast TCP and UDP protocols

References:

Cisco > Home > Internetworking Technology Handbook > Internet Protocols > User Datagram Protocol (UDP)

Licensed to Berend Post berend.post@it-university.nl

Question 84

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

- ☐ ICMP redirect message
- ☒ ICMP echo-request message
- ☐ ICMP time-exceeded message
- ☐ ICMP destination-unreachable message

Explanation:

Explanation:

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

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Cisco > Internetworking Technology Handbook > Internet Protocols (IP)

Licensed to Berend Post berend.post@it-university.nl

Question 85

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

- ☐ Split horizon
- ☒ Spanning Tree Protocol (STP)
- ☐ Holddowns
- ☐ Route poisoning

Explanation:

Explanation:

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

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

Router A 192.168.5.1/24

Router B 192.168.5.2/24

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

routerA# show ip route

Gateway of last resort is 192.168.5.2 to network 0.0.0.0

<Output omitted>

routerB# show ip route

Gateway of last resort is 192.168.5.1 to network 0.0.0.0

<<output omitted>>

From the limited information shown above, you can see that Router A is pointing to Router B for the default route, and Router B is pointing to Router A for the default route. This will cause a routing loop for any traffic that is not in their routing tables. For example, if a ping were initiated to the address 103.5.6.8 and that address was not in the routing tables of Routers A and B, the most likely

Licensed to Berend Post berend.post@it-university.nl

message received back would NOT be "destination unreachable" but "TTL expired in transit." This would be caused by the packet looping between the two routers until the TTL expired.

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

Split horizon stops routing loops by preventing route update information from being sent back over the same interface on which it arrived.

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

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

Question 86

The output of the show ip route command is given:

Router# show ip route

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

What does the value 110 in the output represent?

- ☒ The administrative distance of the information source
- ☐ The metric to the route
- ☐ The type of route
- ☐ The port number of the remote router

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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

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

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

Router# show ip route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O 172.16.0.0 [110/5] via 10.19.24.6, 0:01:00, Ethernet2

B 172.17.12.0 [200/128] via 10.19.24.24, 0:02:22, Ethernet2

O 172.71.13.0 [110/5] via 10.19.24.6, 0:00:59, Ethernet2

O 10.13.0.0 [110/5] via 10.19.24.6, 0:00:59, Ethernet2

The following are the fields in the output:

O: Indicates that the route was discovered using Open Shortest Path First (OSPF).

Licensed to Berend Post berend.post@it-university.nl

B: Indicates that the route was discovered using Border Gateway Protocol (BGP).

172.16.0.0: Indicates the address of the remote network.

110: Indicates the administrative distance of the route.

128: Indicates the metric for the route.

Via 10.19.24.6: Specifies the address of the next router in the remote network.

0:02:22: Indicates the last time the route was updated.

The metric for the route is also called the cost. In the case of the OSPF routes above, the cost is 5.

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

Router(config)# router rip

Router(config)# distance 100

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

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 87

What is the significance of the 1 in the following configuration?

router(config)# router eigrp 1

- ☐ It is the process ID for EIGRP and is locally significant to this router.
- ☐ It is the process ID for EIGRP and must be the same on all EIGRP routers.
- ☐ It is the AS number for EIGRP and is locally significant to this router.
- ☒ It is the AS number for EIGRP and must be the same on all EIGRP routers.

Explanation:

Explanation:

Enhanced Interior Gateway Routing Protocol (EIGRP) configuration requires the specification of an Autonomous System (AS) number with the router eigrp command. Any number can be chosen, but it must match on all EIGRP routers in the domain. This value may appear to be is similar to one used in enabling OSPF, which demands a process ID number but that value is locally significant to each router and need not match on each router.

The syntax of this command is router eigrp [autonomous-system]. Therefore, the 1 in the example indicates an Autonomous System (AS) number, not a process ID.

The Autonomous System (AS) number is not locally significant to each router, and must match on all EIGRP routers.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Licensed to Berend Post berend.post@it-university.nl

Question 88

Which two statements are TRUE of default routes? (Choose two.)

- ☐ Default routes are used for routing packets destined only for networks that are listed in the routing table.
- ☒ Default routes are used for routing packets destined for networks that are not listed in the routing table.
- ☐ Default routes should not be used in a stub network.
- ☒ Default routes are ideal for use in stub networks.
- ☐ Network security is increased by using default routes.

Explanation:

Explanation:

Default routes are to route packets that are destined for networks not listed in the routing table. Also, default routes are ideal for use in stub networks. Stub networks are those that have only one adjacent router interface and therefore only one interface to send any packet, regardless of destination. When used in this fashion the default route will be the only route in the routing table.

The following statements are also true of default routes:

A default route is also known as the gateway of last resort.

The default route in Internet Protocol Version 4 (IPv4) is represented as 0.0.0.0/0.

The option stating that default routes are used to route packets destined only for networks that are listed in the routing table is incorrect. Default routes are used for routing packets that are destined for networks not listed in the routing table.

The option stating that default routes should not be used in a stub network is incorrect. Default routes are helpful in topologies where it is not necessary to learn specific networks, making them ideal for use in a stub network.

The option stating that network security is increased by using default routes is incorrect. Default routes are not concerned with enhancing network security.

Objective:

Routing Fundamentals

Sub-Objective:

Describe the routing concepts

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Technology Support > IP > IP Routing > Design > Design Technotes > Configuring a Gateway of Last Resort Using IP Commands > Document ID: 16448 > Flag a Default Network

Question 89

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

- ☐ TFTP, Flash, ROM
- ☐ ROM, Flash, TFTP
- ☒ Flash, TFTP, ROM
- ☐ Flash, TFTP, NVRAM
- ☐ NVRAM, Flash, TFTP

Explanation:

Explanation:

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

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

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

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 90

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

- ☐ FDDI
- ☐ CDDI
- ☒ SONET
- ☐ Token Ring

Explanation:

Explanation:

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

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

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast network topologies

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 91

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

- ☐ show interface fastethernet0/1 detail
- ☐ show controllers fastethernet0/1
- ☐ show interface fastethernet0/1 status
- ☒ show interfaces fastethernet0/1 switchport

Explanation:

Explanation:

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

switch# show interfaces fastethernet0/1 switchport

Name: Fa0/1

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: Off

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Voice VLAN: none

<<output omitted>>

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

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

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

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

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

Question 92

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

Which command would NOT be useful for discovering the problem?

- ☐ show running-configuration
- ☒ show vlans
- ☐ show standby brief
- ☐ show standby

Explanation:

Explanation:

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

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

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

 Licensed to Berend Post berend.post@it-university.nl

Example A: show running-configuration

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

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

Example B: show standby brief

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

Router C

Interface Grp Prio P State Active addr Standby addr Group addr

Fa0/1 102 200 Active local 10.10.10.253 10.10.10.251

Router D

Interface Grp Prio P State Active addr Standby addr Group addr

Fa0/1 102 200 P Active local 10.10.10.253 10.10.10.251

 Licensed to Berend Post berend.post@it-university.nl

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

Example C: show standby

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

```
Router E

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

Router F

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

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

 Licensed to Berend Post berend.post@it-university.nl

will decrement its priority (190) by 50 as shown in last two lines of its output, leaving the priority at 140. Therefore, to ensure that Router F maintains its role as active even after the dual shutdowns, the priority of Router F should be increased to at least 241. When both routers decrement their priorities after shutdown, Router F will then have a priority of 191, which will be higher than the priority value of Router E.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks

Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands

Question 93

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

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

- ☒ configure an IP SLA responder on the destination device
- ☐ configure an IP SLA responder on the source device
- ☐ schedule the operation on the destination device
- ☐ add the verify-data command to the configuration of the operation

Explanation:

Explanation:

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Infrastructure Management

Sub-Objective:

Troubleshoot network connectivity issues using ICMP echo-based IP SLA

References:

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

Question 94

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

- ☐ Requires a hierarchical physical topology
- ☒ Does not require a hierarchical physical topology
- ☒ Uses Diffusing Update Algorithm (DUAL) to provide loop prevention
- ☐ Uses Bellman-Ford algorithm to provide loop prevention
- ☒ Supports Message-Digest Algorithm 5 (MD5) authentication
- ☐ Does not support Message-Digest Algorithm 5 (MD5) authentication
- ☒ Can differentiate between internal and external routes
- ☒ Uses a 32-bit metric

Explanation:

Explanation:

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

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

Supports large networks due to high scalability

Provides fast convergence using the Diffusing Update Algorithm (DUAL)

 Licensed to Berend Post berend.post@it-university.nl

Performs equal and unequal load balancing by default

Supports variable length subnet masks (VLSM) and classless interdomain routing (CIDR)

Is a hybrid routing protocol (distance-vector protocol) that also provides link-state protocol characteristics

Is a classless protocol

Sends partial route updates only when there are changes, reducing bandwidth usage for routing updates

Has an administrative distance of 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes

Is used only with Cisco platforms

Provides support for IP IPX and AppleTalk protocols

Can differentiate between internal and external routes

Uses a 32-bit metric

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Cisco > Internetworking Technology Handbook > Enhanced Interior Gateway Routing Protocol (EIGRP)

Licensed to Berend Post berend.post@it-university.nl

Question 95

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

- ☐ Anti-DDoS guard
- ☐ Scatter tracing
- ☒ Access control lists (ACLs)
- ☐ Flow control
- ☒ Rate limiting

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Support > Technology Support > Security and VPN > Authentication Protocols > Technology Information > Technology White Paper > Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks > Document ID: 13634

Question 96

Examine the following output from SwitchD.

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

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

- ☒ switchport mode trunk
- ☐ switchport mode nonegotiate
- ☐ switchport trunk encapsulation 802.1q
- ☐ switchport trunk native VLAN

Explanation:

Explanation:

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

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

Licensed to Berend Post berend.post@it-university.nl

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

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

For this example, the following statements are true:

The trunk link connects to Fa0/0 on the router and Fa0/1 on the switch.

The physical interface F0/0 on the router has been divided into two subinterfaces, Fa0/0.1 and Fa0/0.2.

The encapsulation type of 802.1q has been specified on the two subinterfaces of the router.

The physical interface on the switch has been specified as a trunk link.

The IP addresses 192.168.10.1 and 192.168.20.1 should be the default gateways of the computers located in VLANs 1 and 2, respectively.

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot inter-VLAN routing

References:

 Licensed to Berend Post berend.post@it-university.nl

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

Question 97

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?

- ☒ It may cause broadcast storms.
- ☐ All ports on both switches may change to a forwarding state.
- ☐ It may cause a collision storm.
- ☐ These switches will not forward VTP information.

Explanation:

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

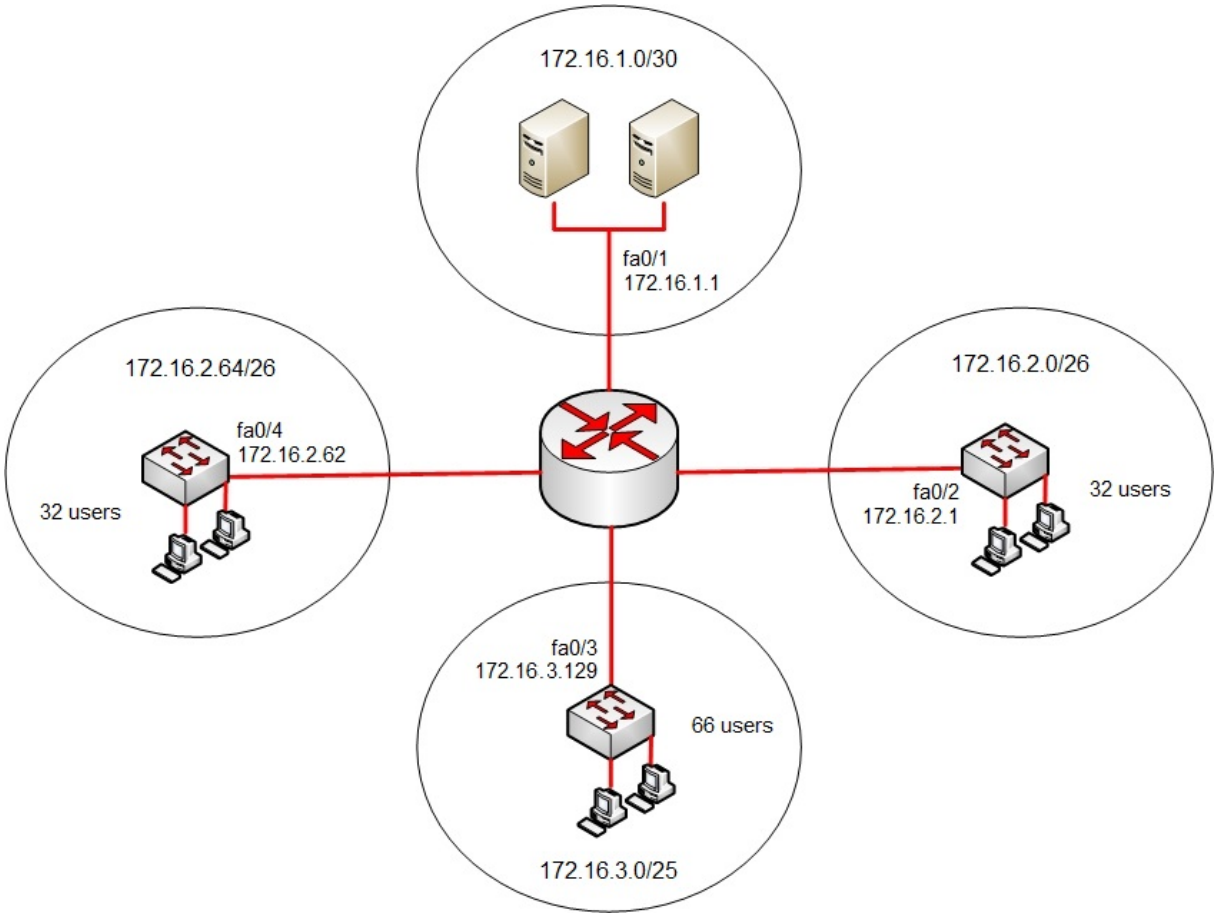
Licensed to Berend Post berend.post@it-university.nl

References:

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

Question 98

Your company's network must make the most efficient use of the IP address space. In the following diagram, the circles define separate network segments. The requirements of each network segment are given in the diagram. (Click the Exhibit(s) button.)



Users complain of connectivity issues. You need to discover the problems with the network configuration.

What are the three problems with the network diagram? (Choose three.)

- ☒ The 172.16.1.0/30 segment requires more user address space.
- ☐ The 172.16.2.0/26 segment requires more user address space.
- ☐ The 172.16.3.0/25 segment requires more user address space.
- ☐ The 172.16.2.64/26 segment requires more user address space.
- ☐ Interface fa0/2 has an IP address that belongs to the 172.16.2.64/26 segment.
- ☒ Interface fa0/4 has an IP address that belongs to the 172.16.2.0/26 segment.
- ☒ Interface fa0/3 has an IP address outside the 172.16.3.0/25 segment.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The given exhibit has three problems:

The 172.16.1.0/30 segment requires more user address space.

Interface Fa0/4 has an IP address that belongs to the 172.16.2.0/26 segment.

Interface Fa0/3 has an IP address outside the 172.16.3.0/25 segment.

The 172.16.1.0/30 segment, as configured, will only support two hosts. This segment needs to support three hosts, the two servers, and the Fa0/1 interface. The number of hosts that a subnet is capable of supporting is a function of the number of host bits in the subnet mask. When that has been determined, the following formula can be used to determine the number of hosts yielded by the mask:

2n - 2 = X

(where n = the number of host bits in the mask and X = the number of hosts supported)

In this example with a 30-bit mask, 2 host bits are left in the mask. When that is plugged into the formula, it yields only two usable addresses. The -2 in the formula represents the two addresses in each subnet that cannot be assigned to hosts, the network ID and the broadcast address. Therefore, the segment should be configured with the 172.16.1.0/29 address range, which supports up to six hosts.

Interface fa0/4, as configured, has an IP address that belongs to the 172.16.2.0/26 segment. With a 26-bit mask and the chosen class B address, the following network IDs are created:

172.16.0.0

172.16.0.64

172.16.1.128

172.16.1.192

172.16.2.0

172.16.2.64

172.16.2.128

172.16.2.192

172.16.2.0

172.16.2.64

Licensed to Berend Post berend.post@it-university.nl

172.16.2.128

172.16.2.192

...and so on, incrementing each time by 64 in the last octet

The 172.16.2.0/26 segment is allocated host addresses in the 172.16.2.1 through 172.16.2.62 range (the last address, 172.16.2.63, is the broadcast address and cannot be assigned). Interface fa0/4 should be assigned an IP address in the 172.16.2.64/26 range, which includes host addresses in the 172.16.2.65 through 172.16.2.126 range.

Interface Fa0/3, as configured, has an IP address outside the 172.16.3.0/25 segment. With a 25-bit mask and the chosen class B address, the following network IDs are created:

172.16.0.0

172.16.0.128

172.16.1.0

172.16.1.128

172.16.2.0

172.16.2.128

172.16.3.0

172.16.3.128

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

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

The 172.16.2.0/26 segment does not require more user address space. With a 26-bit mask, 6 bits are left for hosts, and by using the above formula it can be determined that it will yield 62 hosts. It requires 32.

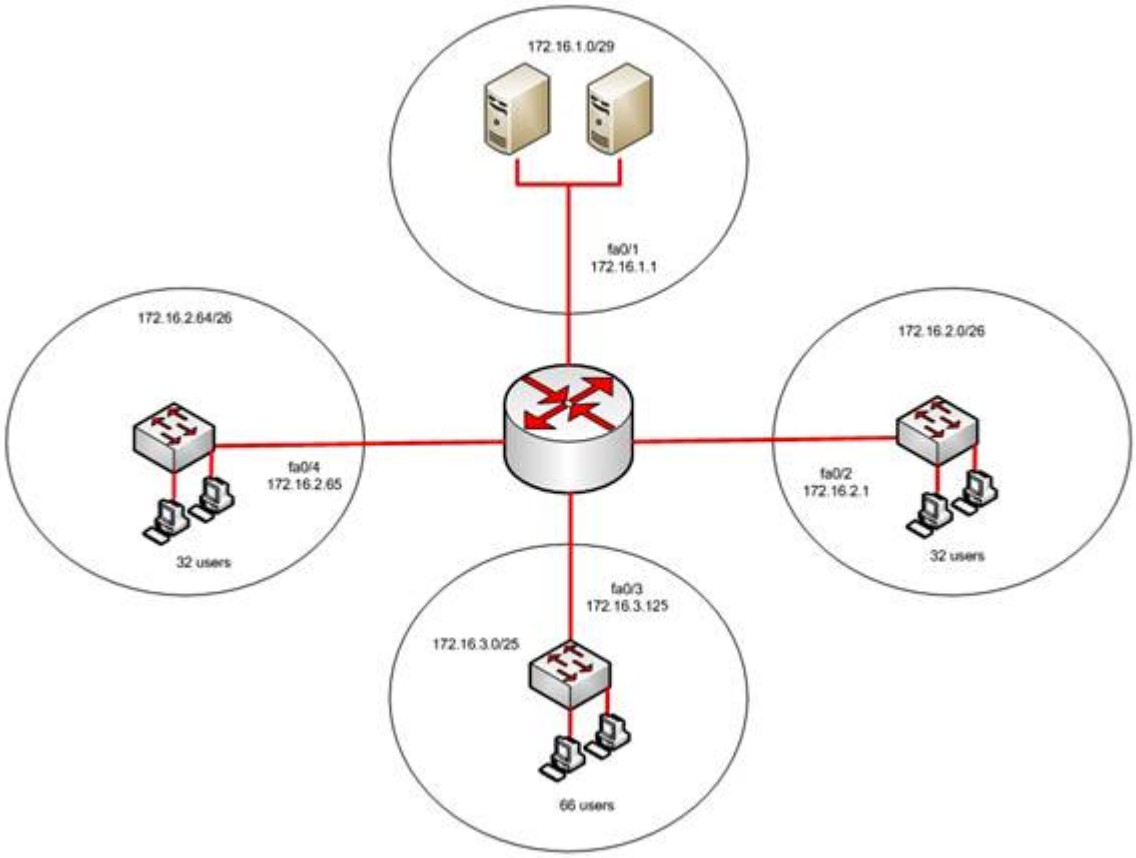
The 172.16.2.64/26 segment does not require more user address space. With a 26-bit mask, 6 bits are left for hosts, and by using the above formula it can be determined that it will yield 62 hosts. It requires 32.

Interface Fa0/2 does not have an IP address that belongs to the 172.16.2.64/26 segment. The 172.16.2.64/26 segment includes addresses 172.16.2.65-172.16.5.126. Because its address is

Licensed to Berend Post berend.post@it-university.nl

172.16.2.1, it belongs in the 172.16.2.0/26 network (from 172.16.2.1-172.16.2.62), so it is correctly configured.

The network should be configured as shown in the following image:



Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

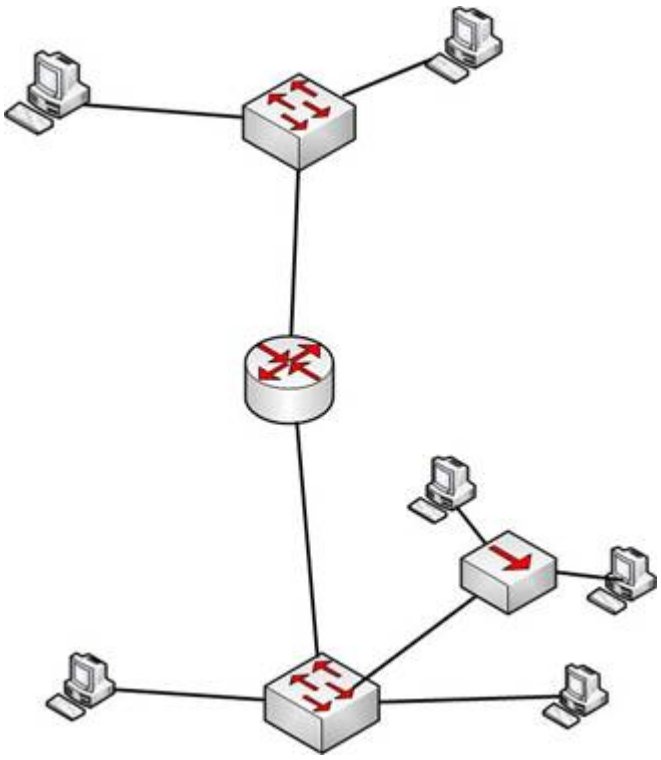
References:

IP Addressing and Subnetting for New Users

Licensed to Berend Post berend.post@it-university.nl

Question 99

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



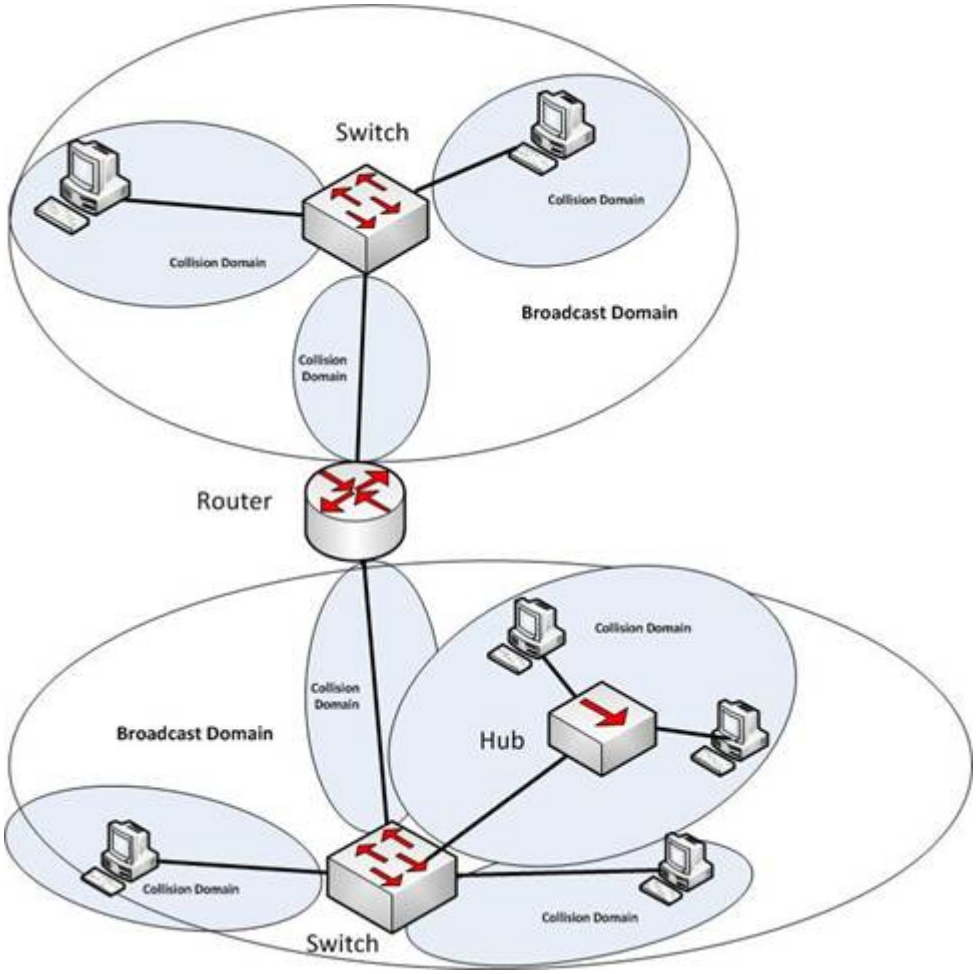
- ☐ 4 collision domains and 3 broadcast domains
- ☒ 7 collision domains and 2 broadcast domains
- ☐ 8 collision domains and 1 broadcast domain
- ☐ 6 collision domains and 2 broadcast domains

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl



Objective:

Routing Fundamentals

Sub-Objective:

Describe the routing concepts

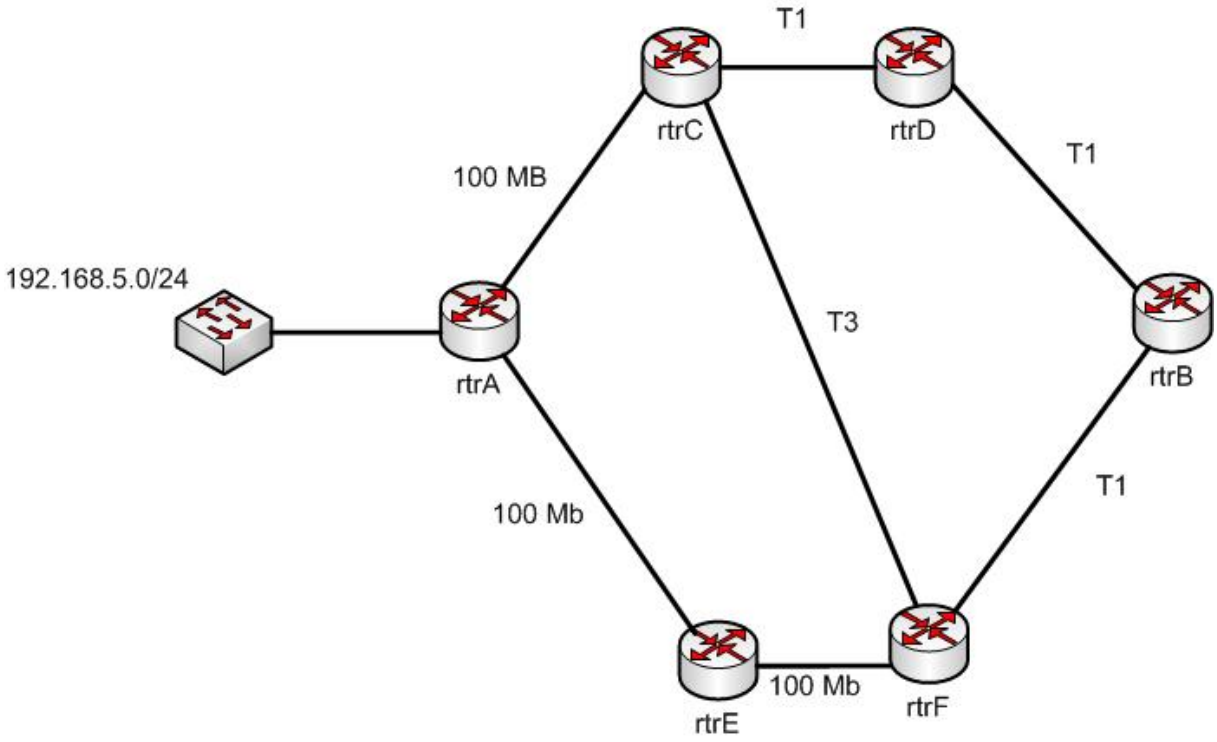
References:

Internetwork Design Guide -- Designing Switched LAN Internetworks > Comparison of LAN Switches and Routers

Licensed to Berend Post berend.post@it-university.nl

Question 100

Examine the following diagram:



While troubleshooting an OSPF routing problem, you need to determine the cost for Router F to reach the 192.168.5.0 24 network via the best route.

What will that cost be?

- ☐ 110
- ☒ 2
- ☐ 3
- ☐ 7

Explanation:

Explanation:

The best route to the 192.168.5.0/24 network from the perspective of router F will have an OSPF assigned cost of 2. There are three possible loop-free paths to get from router F to the 192.168.5.0/24 network. The default OSPF costs for a 100 MB link, a T1 link, and a T3 link are 1, 64, and 2, respectively.

The three paths and the calculation of their costs are shown:

Router F to Router E to Router A: 1 + 1 = 2

Router F to Router C to Router A: 2 + 1 = 3

Router F to Router B to Router D to Router C to Router A: 64 + 64 + 64 + 1 = 193

Licensed to Berend Post berend.post@it-university.nl

Each OSPF route calculates the cost of its path to a network, and passes that value on to the next router, which will then add to it the cost to reach that neighbor. For example, the routing table of Router E would look like this for the route to 192.168.5.0/24:

O 192.168.5.0 [110/1] via <output omitted>

Router F would add its own cost to reach Router E to the cost of reaching 192.168.5.0/24, resulting in the following output:

O 192.168.5.0 [110/2] via <output omitted>

110 is the administrative distance of OSPF.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Home > Support > Technology Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > OSPF Cost

Question 101

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?

- ☐ show ip arp
- ☐ debug ip rip
- ☒ show ip protocols
- ☐ show ip routing process
- ☐ show arp
- ☐ show interfaces

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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.

Licensed to Berend Post berend.post@it-university.nl

```
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.

Licensed to Berend Post berend.post@it-university.nl

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

router# show arp

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.0.0.3 0 0004.dd0c.ffcb ARPA Ethernet01

Internet 10.0.0.1 - 0004.dd0c.ff86 ARPA Ethernet0

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

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

router# show interfaces

Ethernet 0 is up, line protocol is up

Hardware is MCI Ethernet,address is 0000.0c00.750c(bia 0000.0c00.750c)

Internet address is 10.108.28.8, subnet mask is 255.255.255.0

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

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Cisco > Cisco IOS IP Routing Protocols Command Reference > IP Routing Protocol-Independent Commands: S through T > show ip protocols

Licensed to Berend Post berend.post@it-university.nl

Question 102

Router 5 has four interfaces. The networks hosted on each interface are as follows:

Fa0/1 192.168.5.4/29
Fa0/2 192.168.6.0/24
Fa0/3 192.168.7.0/24
S0/0 172.16.5.0/24

You execute the following commands on the router:

Router5(config)# router bgp 20
Router5(config-router)# network 192.168.5.0
Router5(config-router)# network 192.168.6.0
Router5(config-router)# network 192.168.7.0
Router5(config-router)# network 172.16.5.0
Router5(config-router)# neighbor 172.16.5.2 remote-as 50
Router5(config-router)# aggregate-address 192.168.5.0 255.255.252.0

After this command sequence is executed, what routes will be present in the routing table of the router at 172.16.5.2? (Choose all that apply.)

- ☒ 192.168.5.4/29
- ☒ 172.16.5.0/24
- ☒ 192.168.6.0/24
- ☒ 192.168.7.0/24
- ☐ none of these will be present
- ☐ only network addresses beginning with 192 will be present

Explanation:

Explanation:

Despite the inclusion of the command aggregate-address 192.168.5.0 255.255.252.0, all subnets of the aggregate route will also be placed in the routing updates because of the omission of the summary-only keyword. Therefore, 192.168.5.4/29, 172.16.5.0/16, 192.168.6.0/24 and 192.168.7.0/24 will be present.

Had the following command been executed, the subnet addresses would not appear in the routing table of the router at 172.16.5.2:

Router5(config-router)# aggregate-address 192.168.5.0 255.255.252.0 summary-only

Therefore, both the aggregate address and all of the 192.168.0.0 subnets will be in the routing table.

Licensed to Berend Post berend.post@it-university.nl

The 172.16.5.0/24 network will be in the routing table of the router at 172.160.5.1 because it is directly connected.

Objective:

WAN Technologies

Sub-Objective:

Configure and verify single-homed branch connectivity using eBGP IPv4 (limited to peering and route advertisement using Network command only)

References:

Cisco > Cisco IOS IP Routing: BGP Command Reference > aggregate-address

Question 103

```
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?

- ☐ tracert 10.10.10.1
- ☐ traceroute 12.1.10.2
- ☐ ping 10.10.10.1
- ☒ ping

Explanation:

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

 Licensed to Berend Post berend.post@it-university.nl

specifying the target IP address. It takes the command into configuration mode, where various parameters, including the destination and target IP addresses, can be defined.

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

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > ping

Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730 > The Extended ping Command

Cisco Documentation > Internetwork Troubleshooting Handbook > Troubleshooting TCP/IP

Licensed to Berend Post berend.post@it-university.nl

Question 104

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

- ☐ DoS
- ☐ DDoS
- ☒ spoofing
- ☐ SYN floods

Explanation:

Explanation:

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

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

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

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

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

Objective:

Infrastructure Security

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > The Internet Protocol Journal, Volume 10, No. 4 > IP Spoofing

Question 105

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

- ☒ store and forward
- ☐ cut-through
- ☐ fragment free
- ☐ frame-forward

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco Documentation > Internetworking Case Studies > LAN Switching

Question 106

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

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

What does "r" represent in this output?

- ☐ Router
- ☐ Route bridge
- ☐ Hub
- ☒ Repeater

Explanation:

Explanation:

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

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

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

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

DevicID Local Intrfce Holdtme Capability Platform Port ID

lab-7206 Eth 0 157 R 7206VXR Fas 0/0/0

 Licensed to Berend Post berend.post@it-university.nl

lab-as5300-1 Eth 0 163 R AS5300 Fas 0

lab-as5300-2 Eth 0 159 R AS5300 Eth 0

lab-as5300-3 Eth 0 122 R AS5300 Eth 0

lab-as5300-4 Eth 0 132 R AS5300 Fas 0/0

lab-3621 Eth 0 140 R S 3631-telcoFas 0/0

008024 2758E0 Eth 0 132 T CAT3000 1/2

lab-400-1 Eth 0 130 r FH400 Fas 0/0

The fields in the output are as follows:

Device ID: The ID, Media Access Control (MAC) address or the serial number of the neighboring device.

Local Intrfce: The protocol which the connectivity media uses.

Holdtme: The time duration for which the CDP advertisement will be held back by the current device from a transmitting router before it gets discarded.

Capability: The type of device discovered by the CDP. It can have the following values:

R Router

T Transparent bridge

B Source-routing bridge

S Switch

H Host

I IGMP device

r Repeater

Platform: The product number of the device.

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Cisco IOS Network Command Reference, Release 12.4 > show cdp neighbors

Question 107

Which commands would be used to enable Enhanced Interior Gateway Routing Protocol (EIGRP) on a router, and configure the IP addresses 10.2.2.2 and 192.168.1.1 as a part of complete EIGRP configuration? (Choose three.)

- ☒ router eigrp 10
- ☐ router eigrp
- ☐ network 10.2.2.2
- ☒ network 10.0.0.0
- ☒ network 192.168.1.0
- ☐ network 192.168.1.1

Explanation:

Explanation:

The router eigrp 10 command is used to enable EIGRP on a router. The network 10.0.0.0 and network 192.168.1.0 commands are used to activate EIGRP over the interfaces configured with IP addresses 10.2.2.2 and 192.168.1.1. If we were given the subnet mask for the two interfaces, we could include that in the network command as well.

The following command sequence is used to configure EIGRP on a router:

router(config) # router eigrp [autonomous-system]

router (config-router) # network x.x.x.x [wildcard-mask]

router (config-router) # network y.y.y.y [wildcard-mask]

 Licensed to Berend Post berend.post@it-university.nl

The autonomous-system parameter of the router eigrp command specifies the autonomous system number. To ensure that all the routers in a network can communicate with each other, you should specify the same autonomous system number on all the routers.

The parameters of the network command are:

x.x.x.x - This is the major (classful) network number connected to the router.

y.y.y.y - This is the other major (classful) network number connected to the router.

If either the AS numbers do not match between two EIGRP routers or one end is not configured with EIGRP, no EIGRP routes will appear in the routing table of either router, because they will not have formed an EIGRP neighbor relationship. In this situation you will be able ping between the routers, but you will not be able to ping LANs attached to the other router.

The router eigrp command is incorrect because you need to specify the autonomous system number after the command to enable EIGRP in a network. The router eigrp 10 command includes the autonomous-system parameter.

The network 192.168.1.1 and network 10.2.2.2 commands are incorrect because the command must be in terms of the network or subnet ID of the network in which the interfaces reside. It is not entered in terms of the address of the interfaces.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Cisco > Support > Cisco IOS Software > Configuring EIGRP > Enabling EIGRP

Licensed to Berend Post berend.post@it-university.nl

Question 108

You are the network administrator for your company. The Chief Technical Officer of the company is looking for a routing solution that satisfies the following requirements:
No routing protocol advertisements
Increased network security
No routing protocol overhead
Not concerned about fault tolerance

Which of the following routing techniques matches the criteria?

- ☐ Dynamic routing
- ☐ Hybrid routing
- ☒ Static routing
- ☐ Public routing

Explanation:

Explanation:

The static routing technique matches the criteria given in this scenario. Static routing is a process of manually entering routes into a routing table. Static routes are not recommended for large networks because static routes are manually configured on the router. However, if a single link is used to connect an enterprise to an Internet Service Provider (ISP), then static routing is the best option.

The following are characteristics of static routing:

Configuring static routes does not create any network traffic.

Manually configured static routes do not generate routing updates and therefore do not consume any network bandwidth.

Router resources are used more efficiently.

Static routes are not recommended for large networks because they are manually configured on the router and maintaining the routes can become problematic.

Static route configuration is not fault tolerant, because static routes do not automatically adapt to changes in the network.

The dynamic routing option is incorrect because route updates consume bandwidth and overhead. While the scenario is not concerned with routing protocol overhead, it states that there should be no bandwidth consumption by route advertisements.

Hybrid routing and public routing are not valid routing techniques in Cisco terminology.

Objective:

Routing Fundamentals

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Compare and contrast static routing and dynamic routing

References:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Algorithm Types

Question 109

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

- ☒ router(config)# enable password cisco
- ☐ router# enable secret cisco
- ☐ router(config)# line password cisco
- ☐ router(config-router)# enable password cisco

Explanation:

Explanation:

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

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

The parameters of the command are as follows:

level level: An optional parameter to set the privilege level at which the password applies. The default value is 15.

password: Specifies the password that is used to enter enable mode.

encryption-type: An optional parameter to specify the algorithm used to encrypt the password.

encrypted-password: Specifies the encrypted password that is copied from another router configuration.

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

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

 Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Cisco IOS Security Command Reference > E > enable password

Cisco > Cisco IOS Security Configuration Guide, Release 12.4 > Part 7: Secure Infrastructure > Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Question 110

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

- ☒ Presentation layer
- ☐ Session layer
- ☐ Application layer
- ☐ Physical layer

Explanation:

Explanation:

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

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

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

 Licensed to Berend Post berend.post@it-university.nl

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

The three remaining layers in the OSI model are the Transport, Network, and Data Link layers. The Transport layer is responsible for error-free and sequential delivery of data. This layer is used to manage data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

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

The seven layers of the OSI model are sequentially interconnected to each other. From the top to the bottom, the seven layers are:

Layer 7: Application

Layer 6: Presentation

Layer 5: Session

Layer 4: Transport

Layer 3: Network

Layer 2: Data Link

Layer 1: Physical

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast OSI and TCP/IP models

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 111

Which protocol is responsible for negotiating and maintaining Point-to-Point Protocol (PPP) connections?

- ☒ LCP
- ☐ NCP
- ☐ BRI
- ☐ ISDN

Explanation:

Explanation:

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

Authentication method used (PAP or CHAP), if any

Compression algorithm used (Stacker or Predictor), if any

Callback phone number to use, if defined

Multilink; other physical connections to use, if configured

The ability to utilize compression, authentication, and multilink are three options that make PPP a popular choice for Layer 2 encapsulation over a WAN link.

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

In summary, the three steps in the establishment of a PPP session are:

Link establishment phase

Optional authentication phase

Network layer protocol phase

Basic Rate Interface (BRI) and Integrated Services Digital Network (ISDN) are not components of PPP, so these options are incorrect. BRI is a type of ISDN connection that contains three circuits, two 64K B or bearer channels, and one D or Delta channel. ISDN circuits are a type of WAN connection.

Objective:

 Licensed to Berend Post berend.post@it-university.nl

WAN Technologies

Sub-Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

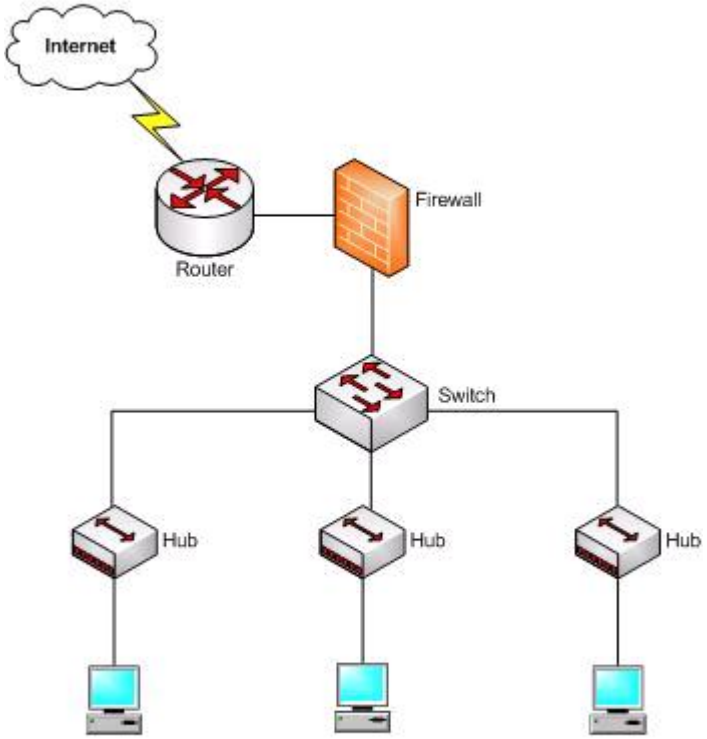
Cisco > Internetworking Technology Handbook > Point-to-Point Protocol

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

Licensed to Berend Post berend.post@it-university.nl

Question 112

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



- ☐ the router
- ☐ the switch
- ☐ the hub(s)
- ☒ the firewall

Explanation:

Explanation:

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

The primary function of a router is to perform routing between two subnets or between dissimilar network technologies. Routers can provide limited firewall functionality, but a firewall is a dedicated

Licensed to Berend Post berend.post@it-university.nl

hardware or software solution with the primary responsibility of securing the network. A router does not have as its primary responsibility the regulation of network traffic flow based on different trust levels.

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

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

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

References:

Cisco > Home > Internetworking Technology Handbook > Internetworking Basics> Bridging and Switching Basics

Question 113

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

- ☐ static
- ☐ override
- ☒ overload
- ☐ dynamic

Explanation:

Explanation:

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

For example:

ip nat pool test 172.28.15.1 172.28.15.1 prefix 24

Licensed to Berend Post berend.post@it-university.nl

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

ip nat inside source list 3 interface serial 0 overload

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

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

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

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

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

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot inside source NAT

References:

Cisco > Technology Support > IP > IP Routing > Design Technotes > Configuring Network Address Translation: Getting Started > Document ID: 13772 > Quick Start Steps for Configuring and Deploying NAT

Question 114

Which statement best describes a converged network?

- ☐ a network with real-time applications
- ☒ a network with a mix of voice, video, and data traffic
- ☐ a network with a mix of voice and video traffic
- ☐ a network with mix of data and video traffic

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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

Converged networks frequently face the following problems:

Bandwidth: As all the voice and video networks are combined into one universal converged network, bandwidth capacity becomes a priority.

Packet loss: When links become congested, packets will be dropped. Voice and video traffic are intolerant of dropped packets.

Delay: Delay represents the time it takes for packets to traverse the network and reach their destinations. While some delay is expected, delay increases when links are over-subscribed.

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast network topologies

References:

Cisco Documentation > Internetworking Technology Handbook > Multiservice Access Technologies

Licensed to Berend Post berend.post@it-university.nl

Question 115

Refer to the following configuration on a Cisco router to allow Telnet access to remote users:

Router(config)#line vty 0 2
Router(config-line)#login
Router(config-line)#password guest

How many users can Telnet into this router at the same time?

- ☐ 0
- ☐ 1
- ☐ 2
- ☒ 3
- ☐ 5

Explanation:

Explanation:

The given configuration will allow three users to Telnet into the router at the same time. The line vty 0 2 command specifies a range from 0 to 2; therefore, three simultaneous Telnet sessions are allowed on this Cisco router. The commands in the exhibit can be explained as follows:

Router(config)#line vty 0 2 (determines which of the five possible terminal lines are being configured. In this case, they are lines 0 through 2. It also determines the number of lines available, in that any line with no password configured will be unusable.)

Router(config-line)#login (specifies that a password will be required)

Router(config-line)#password guest (specifies the password)

The default configuration allows five simultaneous Telnet sessions on the Cisco router. For the default configuration, you would issue the vty 0 4 command in global configuration mode.

You must configure a password when enabling a router for Telnet access. Without a password, the login access to the router will be disabled and you will receive the following error message if you try to Telnet to the router:

router# telnet 10.10.10.1

Trying 10.10.10.1 ... Open

Password required, but none set

[Connection to 10.10.10.1 closed by foreign host]

 Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device management

References:

Question 116

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

- ☐ 172.16.2.1 - 172.16.4.254
- ☐ 172.16.3.1 - 172.16.5.254
- ☒ 172.16.4.1 - 172.16.5.254
- ☐ 172.16.4.1 - 172.16.4.254

Explanation:

Explanation:

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

To determine the range of addresses that can be assigned in a subnet, you must first determine the network ID and broadcast address of the subnetwork. All addresses that can be assigned to hosts will lie between these two endpoints. The network ID can be obtained by determining the interval between subnet IDs. With a 23-bit mask, the decimal equivalent of the mask will be 255.255.254.0. The interval between subnets can be derived by subtracting the value of the last octet of the mask from 256. In this case that operation would be 256 - 254. Therefore, the interval is 2, and it is applied in the third octet where the subnet mask ends.

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

172.16.0.0

172.16.2.0

172.16.4.0

172.16.6.0

Licensed to Berend Post berend.post@it-university.nl

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

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

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

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

Question 117

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

- ☐ variable length subnet masks (VLSM)
- ☐ partial updates
- ☐ neighbor discovery mechanism
- ☒ multiple vendor compatibility

Explanation:

Explanation:

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

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

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

EIGRP routers send partial updates when there are network events.

The following are features offered by EIGRP:

 Licensed to Berend Post berend.post@it-university.nl

Fast convergence

Partial updates

Neighbor discovery mechanism

VLSM

Route summarization

Scalability

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

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

Question 118

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

- ☒ router(config)# ip route 192.168.11.0 255.255.255.0 192.168.43.1
- ☐ router# ip route 192.168.11.0 255.255.255.0 192.168.43.1
- ☐ router(config)# ip classless 192.168.43.1
- ☐ router(config)# ip default gateway 192.168.11.0 255.255.255.0 192.168.43.1
- ☐ router# ip default gateway 192.168.43.1

Explanation:

Explanation:

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

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

The parameters of the command are as follows:

 Licensed to Berend Post berend.post@it-university.nl

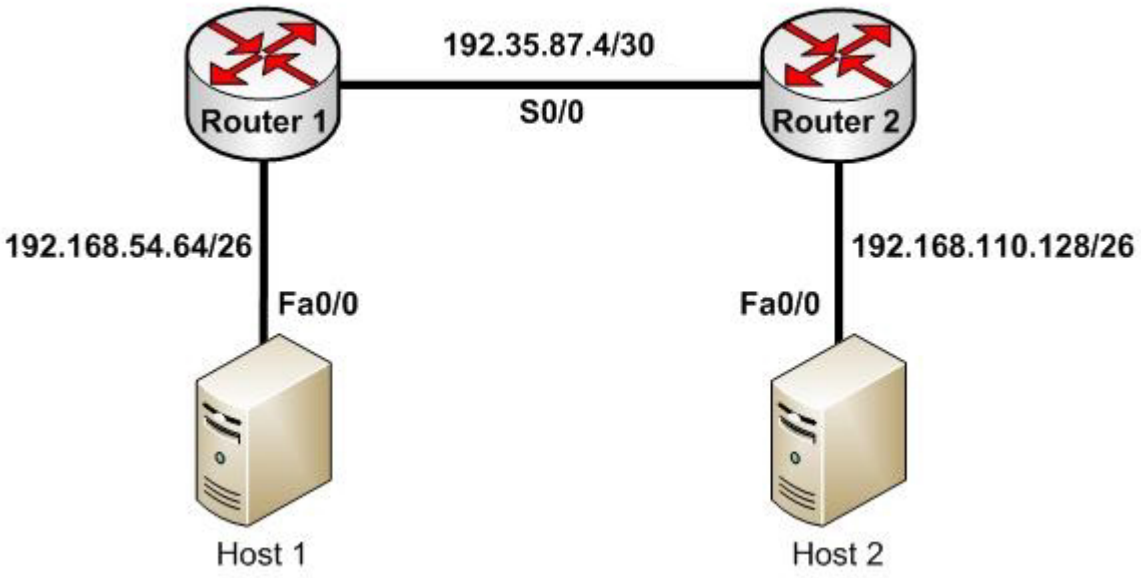
destination_network: Defines the network that needs to be added in the routing table.

mask: Defines the subnet mask used on the network.

next-hop_address: Defines the default gateway or next hop router that receives and forwards the packets to the remote network.

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

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



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

<output omitted>

interface Fa0/1

Licensed to Berend Post berend.post@it-university.nl

```
    ip address 192.168.54.65 255.255.255.192
    no shutdown
interface S0/0
    ip address 192.35.87.5 255.255.255.252
    no shutdown
```

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

Cisco > Cisco ASDM User Guide, 6.1 > Configuring Dynamic And Static Routing > Field Information for Static Routes

Cisco > Support > IP > IP Routing > Design > Design TechNotes > Specifying a Next Hop IP Address for Static Routes > Document ID: 27082

Cisco > Cisco IOS IP Routing Protocols Command Reference > IP Routing Protocol-Independent Commands: A through R > ip route

Licensed to Berend Post berend.post@it-university.nl

Question 119

What IOS command produced the following output?

```
<output omitted>
Vlan Mac Address Type Ports
---- ------------ ------- -----
1 0040.63d8.ba0a DYNAMIC Fa0/1
1 0004.274c.9ca0 DYNAMIC Fa0/3
1 0040.63d8.bab8 DYNAMIC Fa0/10
1 000f.1fd3.d85a DYNAMIC Fa0/7
<output omitted>
```

- ☐ show interface mac
- ☐ show mac
- ☒ show mac-address-table
- ☐ show ip interface

Explanation:

Explanation:

The output was produced by the show mac-address-table command. The show mac-address-table command displays a table of every learned MAC address and the switch port associated with the MAC address. The output shown in the question indicates that four MAC addresses have been learned by this switch, and the last column indicates the switch port over which each MAC address was learned, and for which frames destined for each MAC address will be forwarded. The MAC address table is built dynamically by examining the source MAC address of received frames.

The show ip interface command is a router command, and displays no information on MAC address tables.

The show interface mac and show mac commands are incorrect because they are not valid Cisco IOS commands.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Licensed to Berend Post berend.post@it-university.nl

Question 120

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

- ☐ service-module 56000 clock rate speed
- ☒ service-module 56k clock rate speed
- ☐ bandwidth 56k
- ☐ bandwidth 56000

Explanation:

Explanation:

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

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

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

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 121

You are configuring a serial link between a Cisco router and a router produced by another vendor.

What would be the advantages of using Point to Point Protocol (PPP) over High Level Data Link Control (HDLC) in this scenario?

- ☒ HDLC has a proprietary "type" field that may be incompatible with equipment from other vendors.
- ☐ HDLC is not available on non-Cisco routers.
- ☐ PPP is faster.
- ☐ PPP performs error checking.

Explanation:

Explanation:

High Level Data Link Control (HDLC) has a proprietary "type" field that may be incompatible with equipment from other vendors. It is recommended that PPP always be used when combining equipment from multiple vendors because this Data Link layer WAN protocol is an industry standard. PPP is implemented in the same manner on all PPP-capable equipment.

HDLC is available on non-Cisco routers. However, the Cisco implementation has a "type" field that may prevent the connection from working.

PPP is not faster than HDLC.

PPP performs error checking, but so does HDLC.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco > Internetworking Technology Handbook > Point to Point Protocol (PPP)

Licensed to Berend Post berend.post@it-university.nl

Question 122

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

- ☐ switch(config)# vtp domain MARKETING 25
- ☒ switch(config)# vlan 25
- ☒ switch(config-vlan)# name MARKETING
- ☐ switch(config-if)# vlan 25 name MARKETING
- ☐ switch(config)# vtp 25
- ☐ switch(config-vtp)# name MARKETING

Explanation:

Explanation:

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

switch(config)# vlan 25

switch(config-vlan)# name MARKETING

The steps to add anew VLAN are as follows:

Create the new VLAN

Name the VLAN

Add the desired ports to the VLAN

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

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

References:

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

Question 123

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

- ☒ cost
- ☐ administrative distance
- ☐ composite metric
- ☐ hop count

Explanation:

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:

 Licensed to Berend Post berend.post@it-university.nl

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

References:

Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > Route Selection in Cisco Routers

Question 124

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

- ☒ E-mail
- ☐ FTP
- ☐ Web browser
- ☐ Telnet

Explanation:

Explanation:

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

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast TCP and UDP protocols

 Licensed to Berend Post berend.post@it-university.nl

References:

Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems>OSI Model Application Layer

Question 125

Which service is denoted by TCP/UDP port number 53?

- ☒ Domain Name Service (DNS)
- ☐ File Transfer Protocol (FTP)
- ☐ Telnet
- ☐ HTTP

Explanation:

Explanation:

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port number 53 is assigned to Domain Name Service (DNS), which is used to convert hostnames into Internet Protocol (IP) addresses.

Some common TCP and UDP port number assignments are as follows:

port 25: Assigned to Simple Mail Transfer Protocol (SMTP), a TCP protocol used to send and receive e-mail messages.

port 23: Assigned to Telnet to allow remote logins and command execution.

port 21: Assigned to File Transfer Protocol (FTP). It is used to control FTP transmissions. Port number 20 is also used by FTP for FTP data.

port 80: Assigned to Hypertext Transfer Protocol (HTTP), which is the base for transferring Web pages over the Internet.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering

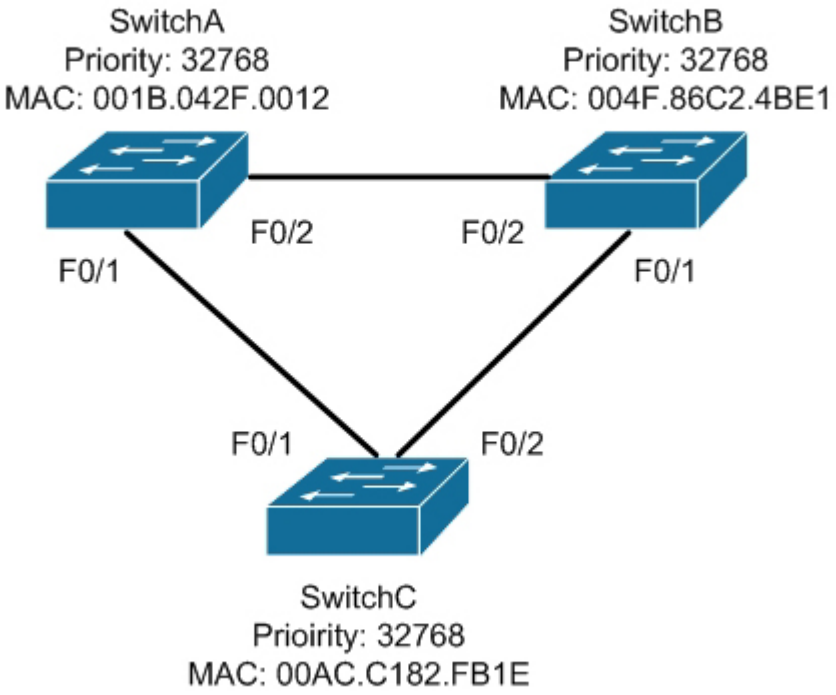
References:

Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems>Multiplexing Basics

Licensed to Berend Post berend.post@it-university.nl

Question 126

View the following network diagram:



Which switch will become the root bridge?

- ☒ SwitchA
- ☐ SwitchB
- ☐ SwitchC
- ☐ The root bridge cannot be determined from the given information.

Explanation:

Explanation:

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

Switch's priority number: Configured as 32768 on Cisco switches by default

Switch's Media Access Control (MAC) address: The burnt-in hardware address of the network interface card

The switch with the lowest bridge ID is selected as the root bridge. If the same priority number is configured on two or more switches in the network, the switch with the lowest MAC address will become the root. Bridge Protocol Data Units (BPDUs) communicate the details of the switch with the lowest bridge ID in the network. The election process for the root bridge takes place every time there is a topology change in the network. A topology change may occur due to the failure of a root bridge or the addition of a new switch in the network. The root bridge originates BPDUs every two seconds,

Licensed to Berend Post berend.post@it-university.nl

which are propagated by other switches throughout the network. BPDUs are used as keepalives between switches, and if a switch stops receiving BPDUs from a neighboring switch for ten intervals (20 seconds), it will assume a designated role for the network segment.

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

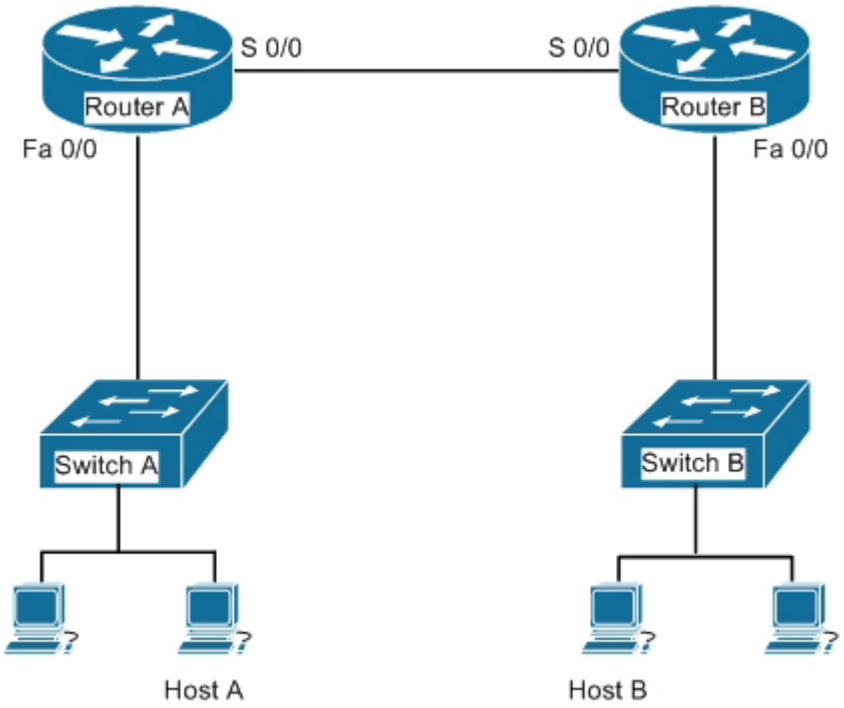
Cisco Documentation > Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX > Configuring STP and IEEE 802.1s MST > Understanding the Bridge ID

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

Licensed to Berend Post berend.post@it-university.nl

Question 127

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



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

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

- ☒ The IP address of Host A and the IP address of the Fa0/0 interface of Router A
- ☐ The IP address of the Fa0/0 interface of Router A and the IP address of the Fa0/0 interface of Router B
- ☐ The IP address of Host A and the IP address of the Fa0/0 interface of Router B
- ☐ The IP address of Host A and the IP address of Switch A
- ☒ The IP address of the S 0/0 interface of Router A and the IP address of the S 0/0 interface of Router B
- ☐ The IP address of Host A and the IP address of Host B
- ☒ The IP address of Host B and the IP address of the Fa0/0 interface of Router B

Explanation:

Explanation:

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

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

Moving from Host A to Host B, however, the following links must be in the same subnet:

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

The IP address of the S0/0 interface of Router A and the IP address of the S0/0 interface of Router B

The IP address of Host B and the IP address of the Fa0/0 interface of Router B

Neither of the switch addresses is important to the process.

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

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

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

Question 128

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

- ☐ show cdp
- ☐ show cdp devices
- ☐ show cdp traffic
- ☒ show cdp neighbors detail

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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

```
Tecumsah# show cdp neighbors detail
-------------------------
Device ID: Tacoma
Entry address(es):
IP address: 172.19.169.88
Platform: cisco 7206VXR, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/0/0
Holdtime : 123 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.1(2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
advertisement version: 2
Duplex: half
-------------------------
Device ID: Topeka
Entry address(es):
IP address: 172.19.169.100
Platform: cisco AS5300, Capabilities: Router
<<output omitted>>
```

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

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

Atlanta# show cdp

Global CDP information:

Sending CDP packets every 60 seconds

Sending a holdtime value of 180 seconds

Sending CDPv2 advertisements is enabled

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

Licensed to Berend Post berend.post@it-university.nl

Birmingham# show cdp traffic

Total packets output: 652, Input: 214

Hdr syntax: 0, Chksum error: 0, Encaps failed: 0

No memory: 0, Invalid: 0, Fragmented: 0

CDP version 1 advertisements output: 269, Input: 50

CDP version 2 advertisements output: 360, Input: 25

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

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

Question 129

Which of the following is NOT a benefit of cloud computing to cloud users?

- ☐ On-demand self-service resources provisioning
- ☐ Centralized appearance of resources
- ☐ Highly available, horizontally scaled applications
- ☒ Cost reduction from standardization and automation

Explanation:

Explanation:

Cost reduction from standardization and automation is a benefit that accrues to the cloud provider, not the cloud users. Additional benefits to cloud providers are:

High utilization through virtualization and shared resources

Easier administration

Fail-in-place operations model

Benefits that accrue to cloud users include:

On-demand self-service resources provisioning

Centralized appearance of resources

 Licensed to Berend Post berend.post@it-university.nl

Highly available, horizontally scaled applications

No local backups required

Cloud users can also benefit from new services such as intelligent DNS, which can direct user requests to locations that are using fewer resources.

Objective:

Network Fundamentals

Sub-Objective:

Describe the effects of cloud resources on enterprise network architecture

References:

Cloud and Systems Management Benefits

Question 130

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

- ☐ boot buffersize
- ☐ configure
- ☒ boot config
- ☐ service config

Explanation:

Explanation:

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

boot config device:filename

The parameters of the command are as follows:

Device : Specifies the device that contains the configuration file.

Filename : Specifies the name of the configuration file.

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

Licensed to Berend Post berend.post@it-university.nl

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

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

Objective:

Infrastructure Management

Sub-Objective:

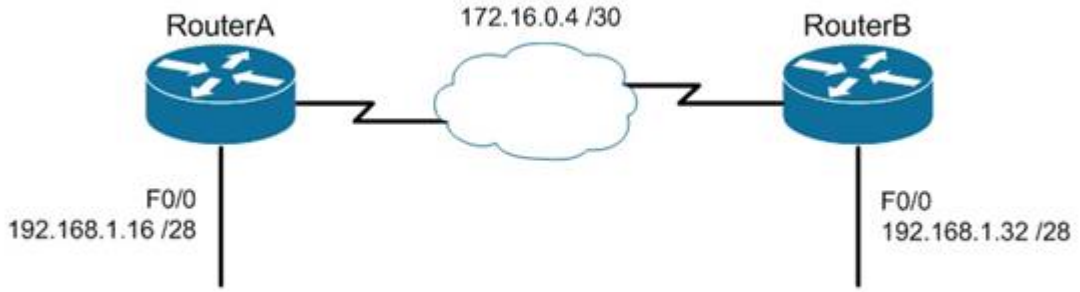
Perform device maintenance

References:

Cisco > Cisco IOS Configuration Fundamentals Command Reference > A through B > boot config

Question 131

Consider the following diagram:



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

- ☒ RIPv1
- ☐ RIPv2
- ☐ EIGRP
- ☐ OSPF

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

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

Question 132

You have added a new router to your network using all of the default settings. You can connect to everything by IP address, but the router doesn't seem to be resolving names to IP addresses. The DNS server is in a directly connected network.

Which of the following is most likely the problem?

- ☒ You configured an incorrect IP address for the DNS server
- ☐ You configured an incorrect default gateway on the router
- ☐ You failed to execute the ip domain lookup command
- ☐ You failed to create an IP helper address

Explanation:

Explanation:

The most likely problem is that you configured an incorrect IP address for the DNS server. Although it is impossible to know without executing the show run command, the other options can all be eliminated, making this the most likely option.

Licensed to Berend Post berend.post@it-university.nl

Even if the router has an incorrect default gateway, or has no default gateway configured, the router should be able to connect to resources by name if it can connect to them by IP address. The gateway will only be required if the DNS server is in a network not found in the routing table of the local router. Since the network containing the DNS server is directly connected, that network is automatically in the routing table.

The ip domain lookup command is enabled by default, so it does not need to be executed. If the scenario had not stated that all defaults were in place, it could be verified with the show run command as shown below, where line 4 indicates the ip domain lookup command is disabled:

routera# show run

<output omitted>

hostname routera

no ip domain lookup

ip domain name acme.com

ip name-server 192.31.1.6

It is not required to have an IP helper address for DNS to function for the router. It is only required by the non-routing devices connected to the router, and only for those that are not on the same network with their DHCP server.

Objective:

Infrastructure Services

Sub-Objective:

Troubleshoot client- and router-based DHCP connectivity issues

References:

Licensed to Berend Post berend.post@it-university.nl

Question 133

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

- ☐ Random access memory (RAM)
- ☐ Flash
- ☒ Non-volatile random access memory (NVRAM)
- ☐ Read-only memory (ROM)

Explanation:

Explanation:

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

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

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

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

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

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

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Cisco IOS Configuration Fundamentals Command Reference > C > copy

Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 8: Managing Configuration Files > Managing Configuration Files

Question 134

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

- ☒ Networks are segmented into multiple collision domains using switches for CSMA/CD networks.
- ☐ Networks are segmented into multiple broadcast domains using switches for CSMA/CD networks.
- ☒ CSMA/CD networks normally operate on half-duplex mode.
- ☐ CSMA/CD networks normally operate on full-duplex mode.
- ☒ Gigabit Ethernet uses CSMA/CD as the media access control method.
- ☐ Gigabit Ethernet uses carrier sense multiple access with collision avoidance (CSMA/CA) as the media access control method.

Explanation:

Explanation:

The following statements are true:

Networks are segmented into multiple collision domains using switches for CSMA/CD networks

CSMA/CD networks normally operate on half-duplex mode

Gigabit Ethernet uses CSMA/CD as its media access control method

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

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

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

 Licensed to Berend Post berend.post@it-university.nl

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Cisco > Internetworking Technology Handbook > Introduction to LAN Protocols > LAN Media-Access Methods

Cisco > The Internet Protocol Journal - Volume 2, No. 3 > Gigabit Ethernet

Question 135

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

- ☒ CSU/DSU
- ☐ switch
- ☒ modem
- ☐ hub

Explanation:

Explanation:

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

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

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies

Question 136

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

- ☐ source IP address
- ☒ source MAC address
- ☐ destination IP address
- ☒ destination MAC address

Explanation:

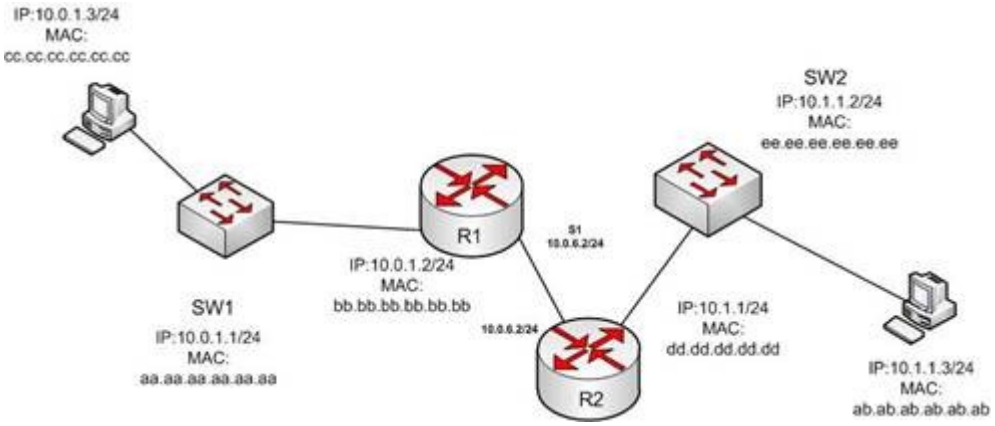
Explanation:

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

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

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

 Licensed to Berend Post berend.post@it-university.nl



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

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

Objective:

Routing Fundamentals

Sub-Objective:

Describe the routing concepts

References:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics

Licensed to Berend Post berend.post@it-university.nl

Question 137

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
```

- ☐ winipcfg
- ☐ ipconfig
- ☐ ifconfig
- ☒ ipconfig/all

Explanation:

Explanation:

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

The router for computer is at 10.88.2.6.

The primary DNS server is 10.88.10.49.

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

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

Licensed to Berend Post berend.post@it-university.nl

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Cisco>Home>Support>Technology Support>IP>IP Addressing Services>Configure>Configuration Examples and TechNotes> Dynamically Configuring DHCP Server Options>Troubleshoot

Question 138

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

- ☐ switch# show standby mac
- ☐ switch# show hsrp mac
- ☒ switch# show standby
- ☐ switch# show standby brief

Explanation:

Explanation:

The command show standby can be used to display the virtual MAC address for HSRP groups of which a switch is a member. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch. The standby switch will take over as the active switch if the timer expires before it hears a heartbeat from the active switch. Below is an example of the show standby command for the HSRP group 1:

Licensed to Berend Post berend.post@it-university.nl

```
Tacoma# show standby

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

In the above output, the following can be determined:

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

```
Router# show standby

Ethernet0/1 - Group 1

  State is Active

   2 state changes, last state change 00:30:59

  Virtual IP address is 10.1.0.20

   Secondary virtual IP address 10.1.0.21

  Active virtual MAC address is 0004.4d82.7981

   Local virtual MAC address is 0004.4d82.7981 (bia)
```

These routers have Ethernet hardware that only recognize a single MAC address. In either case, if for some reason this router becomes the standby router, such as due to loss of interfaces, then when the interfaces come back up it will be able to recover the active role because it is set for preemption, as shown on line 10.

The router is tracking two of its own interfaces. Because both interfaces are down, the router's priority has been reduced by 25 (15 for Fastethernet0/2 and 10 for Fastethernet0/3), from the

 Licensed to Berend Post berend.post@it-university.nl

configured value of 120 to 95. This data is shown on lines 13-16. The default is 10 if not otherwise specified, as is the case for Fastethernet0/3.

If either of the two interfaces comes back up, the priority will be increased by the amount assigned to the interface. For example, if Fastethernet0/3 comes back up, the priority will become 105 (95 + 10).

The standby router is unreachable, which can be determined because it is marked unknown expired in line 12. This could be due to either a physical layer issue or an HSRP misconfiguration.

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

The commands show standby mac and show hsrp mac are invalid due to incorrect syntax.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco > Cisco IOS IP Application Services Command Reference > show standby

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

Question 139

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

- ☐ system LED: no color
- ☐ system LED: solid red
- ☒ system LED: solid amber
- ☐ stat LED: no color
- ☐ stat LED: green

Explanation:

Explanation:

A POST failure is indicated by a solid amber color on the system LED. The switch automatically runs POST which is a series of self-tests to verify proper functioning, after the power is connected. The

 Licensed to Berend Post berend.post@it-university.nl

system LED is off (no color) at the time that POST begins. The LED will turn green if POST is successful, or it will turn amber if POST fails.

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

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

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

Ensure the switch has power

Ensure the proper cable type is in use (for a switch to switch connection use a crossover cable: for a switch to host and or switch to router connection use a straight through)

Ensure a good connection by reseating all cables

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

Layer 1 media is functioning between the switch and the device on the other end of the cable

Layer 2 communication has been established between the switch and the device on the other end of the cable

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot interswitch connectivity

References:

Licensed to Berend Post berend.post@it-university.nl

Question 140

Which Cisco IOS command will display the following partial output?

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

Gateway of last resort is 10.30.10.85 to network 10.71.0.0

E 168.28.0.0 [140/8] via 10.212.215.122, 0:03:34, serial0/0
E 172.43.0.0 [140/8] via 10.145.231.221, 0:43:54, Ethernet 2
```

- ☐ show ip
- ☒ show ip route
- ☐ show ip route summary
- ☐ show route summary

Explanation:

Explanation:

The show ip route command will display the output in this scenario. The command is used to display the present status of the routing table. The complete command syntax is:

show ip route [[ip-address [mask] [longer-prefixes]] | [protocol [process-id]] | [list access-list-number | access-list-name]]

The following is a sample partial output:

D 168.28.0.0 [140/8] via 10.212.215.122, 0:03:34, serial0/0

The first letter represents the routing protocol through which the route is learned. In this case, the route is learned by EIGRP. The command output also lists codes used for all the routing protocols.

The routing protocol code is followed by the IP address of the remote network.

The first number in the bracket represents the administrative distance of the routing protocol. The number followed by slash within the bracket represents the cost of the route. Different routing protocol uses different methods to calculate the cost of the route. The IP address followed by the

 Licensed to Berend Post berend.post@it-university.nl

keyword via shows the next router to the remote network. The next set of numbers is the time when the route was last updated, which is 0:03:34 in the example. Lastly, it displays the interface through which the network can be reached, which is serial0/0 in the example.

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

The show ip route summary command is incorrect because this command is used to view the current state of the routing table.

The show route summary command is incorrect because it is not a valid Cisco IOS command.

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Question 141

You have multiple departments sharing a common network. You are concerned about network traffic from one department reaching another department.

What would be a solution for isolating the departments? (Choose all that apply.)

- ☒ Configure separate VLANs for each department.
- ☐ Assign a unique VTP domain for each department.
- ☐ Put each department in a separate collision domain.
- ☐ Configure trunk links between departmental switches.
- ☒ Configure separate subnets for each department

Explanation:

Explanation:

You could either configure separate VLANs for each department or configure separate subnets for each department. Either approach has the effect of restricting each department's traffic to its local subnet or VLAN, unless you configure and allow inter-VLAN routing.

VLANs logically divide a switched network into multiple independent broadcast domains. Broadcast traffic within one VLAN will never be sent to hosts in other VLANs. In this respect, VLANs operate

 Licensed to Berend Post berend.post@it-university.nl

exactly as subnets do. The only way for hosts in different VLANs to communicate is through a router or multilayer switch configured to perform inter-VLAN routing between the VLANs.

The VLAN Trunking Protocol (VTP) is used to synchronize VLAN databases across multiple switches, and is not a method for isolating departmental traffic.

Collision domains cannot be used to isolate traffic between departments. Multiple departments cannot share a collision domain when using switches. Every port on a switch is a separate collision domain, which allows the switch to forward more than one frame at a time. This also reduces collisions, since each host is therefore in a separate collision domain. The switch processes data based only on MAC addresses, and has no knowledge of which host is in which IP subnet or department.

Trunk links are used to connect switches to other switches and to routers for the purpose of carrying traffic from multiple VLANs, and are not a method of isolating traffic between different departments.

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Cisco > Internetwork Design Guide > Designing Switched LAN Internetworks > Benefits of VLANs

Question 142

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

- ☐ A VTP domain must be configured.
- ☐ VTP pruning should be enabled.
- ☐ The VTP mode of operation should be server.
- ☒ A trunk connection should be set up between the switches.

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

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

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

Question 143

You run the following command:

switch# show ip interface brief

What information is displayed?

- ☐ A summary of the IP addresses and subnet mask on the interface
- ☒ A summary of the IP addresses on the interface and the interface's status
- ☐ The IP packet statistics for the interfaces
- ☐ The IP addresses for the interface and the routing protocol advertising the network

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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

Sample output of this command is shown below:

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

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot interswitch connectivity

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 144

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

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

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

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

- ☐ The passwords are incorrectly configured
- ☐ The usernames are incorrectly configured
- ☒ The wrong interface has been configured
- ☐ The encapsulation is incorrect on RouterA
- ☐ The encapsulation is incorrect on RouterB
- ☐ The authentication types do not match

Explanation:

Explanation:

The two routers are connected using Serial0 on RouterA and Serial1 on RouterB. However, the configuration commands were executed on interface Serial0 on RouterB. So although the configuration itself is completely correct, it is configured on the wrong interface.

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

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

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

Licensed to Berend Post berend.post@it-university.nl

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

RouterB(config-if)#ppp authentication chap pap

Objective:

WAN Technologies

Sub-Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

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

Question 145

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

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

- ☒ ip domain-name
- ☒ transport input ssh
- ☐ ip access-group
- ☒ crypto key generate rsa
- ☐ service config

Explanation:

Explanation:

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

ip domain-name [domain-name]: configures the DNS of the router (global configuration mode)

crypto key generates rsa: generates a cryptographic key to be used with SSH (global configuration mode)

transport input ssh: allows SSH connections on the router's VTY lines (VTY line configuration mode)

 Licensed to Berend Post berend.post@it-university.nl

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

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

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

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

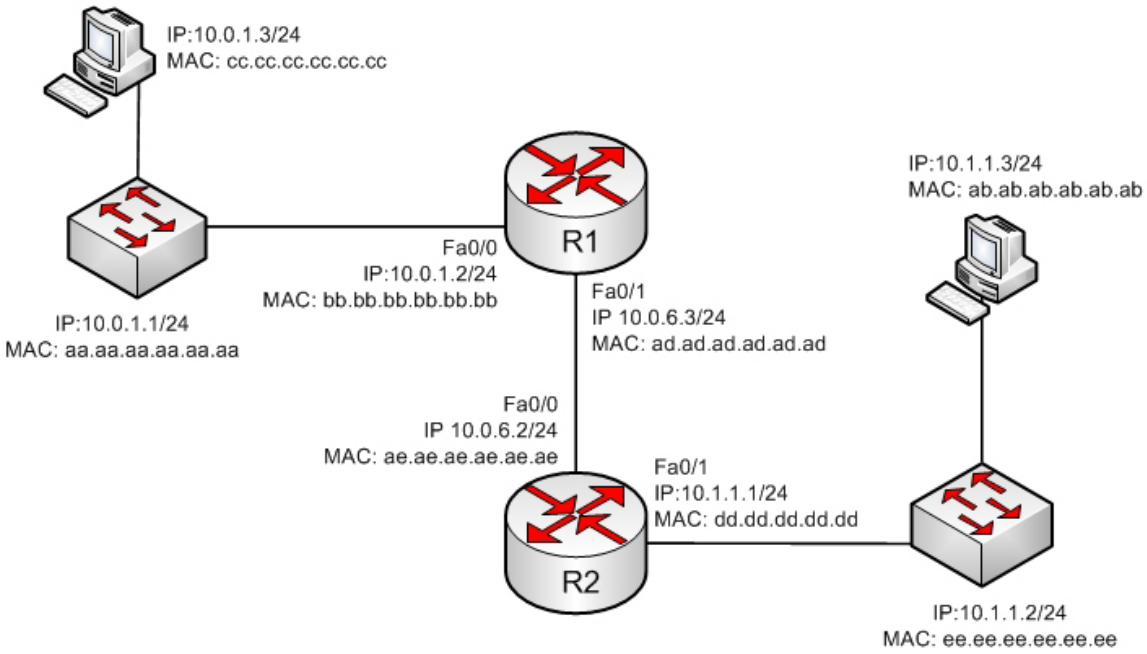
References:

Cisco > Support > Technology Support > Security and VPN > Secure Shell (SSH) > Design > Configuring Secure Shell on Routers and Switches Running Cisco IOS > Document ID: 4145

Licensed to Berend Post berend.post@it-university.nl

Question 146

The workstation at 10.0.1.3 sends a packet to the workstation at 10.1.1.3.



When the packet leaves the R2 router, what addresses will be located in the header? (Choose two.)

- ☐ Source MAC bb.bb.bb.bb.bb.bb Dest MAC ab.ab.ab.ab.ab.ab
- ☒ Source MAC dd.dd.dd.dd.dd.dd Dest MAC ab.ab.ab.ab.ab.ab
- ☐ Source MAC ee.ee.ee.ee.ee.ee Dest MAC ab.ab.ab.ab.ab.ab
- ☒ Source IP 10.0.1.3 Dest IP 10.1.1.3
- ☐ Source IP 10.0.1.1 Dest IP 10.1.1.2
- ☐ Source IP 10.0.1.2 Dest IP 10.1.1.3
- ☐ Source IP 10.0.1.1 Dest IP 10.1.1.3

Explanation:

Explanation:

When the packet leaves the R2 router, the addresses that will be located in the header are:

Source MAC dd.dd.dd.dd.dd.dd

Dest MAC ab.ab.ab.ab.ab.ab

Source IP 10.0.1.3

Dest IP 10.1.1.3

If we executed the ipconfig/all command on the computer located at 10.1.1.3/24, it would look somewhat like what is shown below. The router interface (10.1.1.1/24) would use an ARP broadcast to determine the MAC address associated with the IP address 10.1.1.3/24 and it would be returned

Licensed to Berend Post berend.post@it-university.nl

as ab.ab.ab.ab.ab. The router interface would then encapsulate the packet in a frame addressed to ab.ab.ab.ab.ab.

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

Physical Address. . . . . : AB-AB-AB-AB-AB-AB
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . : fe80::ada3:8b73:a66e:6bc0%10(Preferred)
IPv4 Address. . . . . : 10.1.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, October 14, 2011 12:42:05 PM
Lease Expires . . . . . .: Thursday, October 20, 2011 12:44:20 AM
Default Gateway . . . . . : 10.1.1.1
DHCP Server . . . . . : 10.88.10.48
DHCPv6 IAID . . . . . : 234887840
DHCPv6 Client DUID. . . . : 00-01-00-01-14-EE-0F-98-00-1A-A0-E1-95-AB

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

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Describe the routing concepts

 Licensed to Berend Post berend.post@it-university.nl

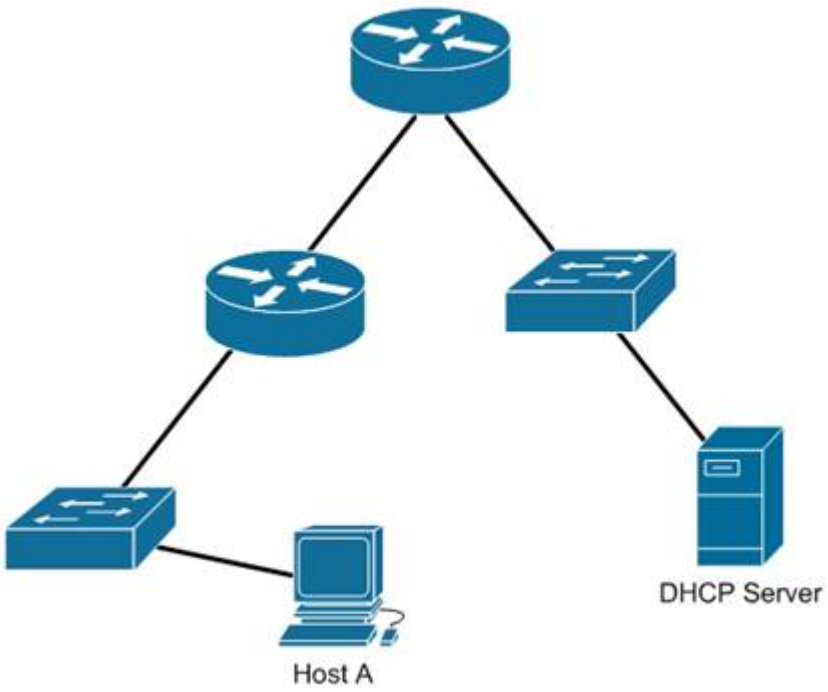
References:

Cisco > IOS Technology Handbook > Routing Basics

Question 147

Host A is configured for DHCP, but it is not receiving an IP address when it powers up.

What is the most likely cause? (Click the Exhibit(s) button to view the network diagram.)



- ☐ The DHCP server is on the wrong subnet.
- ☒ Routers do not forward broadcast traffic.
- ☐ The DHCP server is misconfigured.
- ☐ Port security is enabled on the switch.

Explanation:

Explanation:

Host A is not receiving a DHCP configuration because its initial DHCP Discover frame is a broadcast, and routers do not forward broadcast frames by default.

A DHCP client sends out a DHCP Discover packet when booting up, enveloped within an Ethernet broadcast frame. The broadcast frame will be flooded by switches, but filtered by routers. There

Licensed to Berend Post berend.post@it-university.nl

must either be a DHCP server on the local subnet or a DHCP Relay Agent, which will forward the request from the local subnet to the DHCP server.

The DHCP server is not on the wrong subnet. A DHCP server can be centrally located and configured to support multiple remote subnets, as long as those subnets have DHCP Relay Agents configured to forward the DHCP Discover requests.

No information is provided on the DHCP server configuration. The router is the most obvious cause of the problem, so this option is incorrect.

Port security can be configured to restrict hosts based on the MAC address, but the scenario does not provide information on any port security configurations. The router is the most obvious cause of the problem as shown in the network exhibit.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify DHCP on a router (excluding static reservations)

References:

Cisco > Support > Cisco IOS Software > Configuring the Cisco IOS DHCP Server

Cisco > Support > Cisco IOS Software > Configuring the Cisco IOS DHCP Relay Agent

Question 148

Which of the following are classless routing protocols? (Choose four.)

- ☒ Open Shortest Path First (OSPF)
- ☒ Enhanced Interior Gateway Routing Protocol (EIGRP)
- ☐ Interior Gateway Routing Protocol (IGRP)
- ☐ Routing Information Protocol version 1 (RIPv1)
- ☒ Border Gateway Protocol (BGP)
- ☒ Routing Information Protocol version 2 (RIPv2)

Explanation:

Explanation:

Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), and Routing Information Protocol version 2 (RIPv2) are classless routing protocols.

 Licensed to Berend Post berend.post@it-university.nl

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

The options IGRP and RIPv1 are incorrect because these are classful routing protocols.

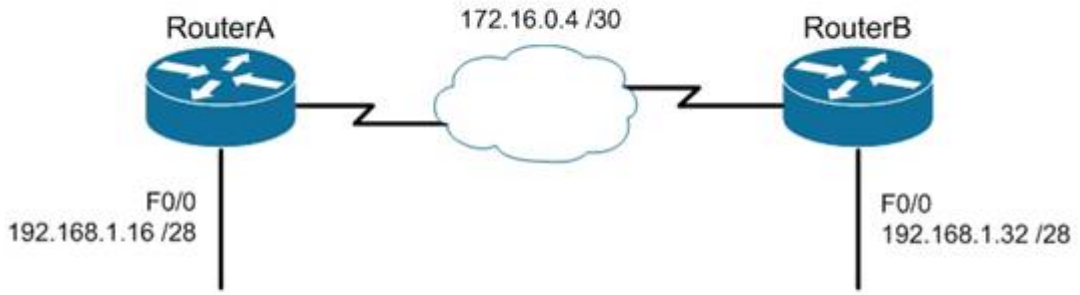
The following are characteristics of classless routing protocols:

The subnet mask is advertised with each route by using classless routing protocols.

Flexible route summarization and supernetting (CIDR) are allowed in classless routing protocols.

Classless routing protocols support variable length subnet masks (VLSM), which allow different subnets of a given IP network to be configured with different subnet masks.

One of the main advantages of using a classless routing protocol is its ability to minimize the effects of discontiguous networks. When subnets of the same classful network are separated by another classful network, the networks are called discontiguous. Examine the diagram below:



The LAN networks extending from Router A and Router B are derived from the same Class C network, 192.168.1.0/24. A classful routing protocol such as RIP v1 would not be able to determine the direction to send the packets, but since classless protocols include the subnet mask in advertisements, they would not suffer the same problem. Whenever networks with non-default subnet masks are used, a classless routing protocol will be required.

Below are some examples of networks that do not have default masks. You can recognize them by the fact that they are not /8, /16, or /24.

Licensed to Berend Post berend.post@it-university.nl

192.168.10.0/27

10.5.6.0/22

172.68.0.0/18

All of the classless protocols discussed here are interior routing protocols with the exception of Border Gateway Protocol (BGP), which is an external routing protocol used to connect different autonomous systems. For example, BGP would be used to connect two OSPF autonomous systems (AS).

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Cisco > Support > IP > IP Routing

Question 149

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

- ☐ Token Ring
- ☐ LocalTalk
- ☐ 100VG-AnyLan
- ☒ Ethernet

Explanation:

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.)

 Licensed to Berend Post berend.post@it-university.nl

CSMA/CD networks normally operate in half-duplex mode, since in a shared collision domain, a host cannot send and receive data at the same time.

CSMA/CD is not required when connected to non-shared (private) collision domains, such as when hosts are connected to dedicated switch ports.

Switches create dedicated collision domains, so devices can operate in full-duplex mode.

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

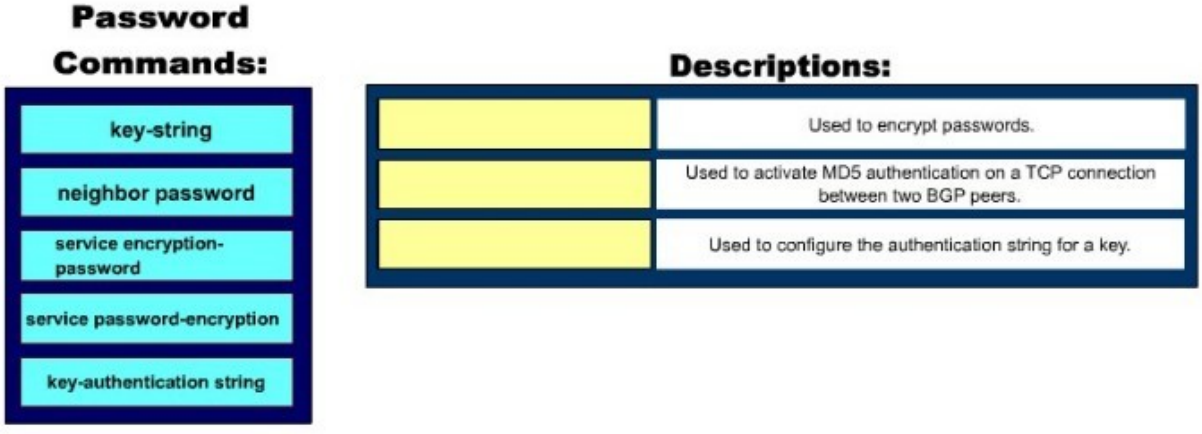
Interpret Ethernet frame format

References:

Cisco > Internetworking Technology Handbook > Introduction to LAN Protocols > LAN Media-Access Methods

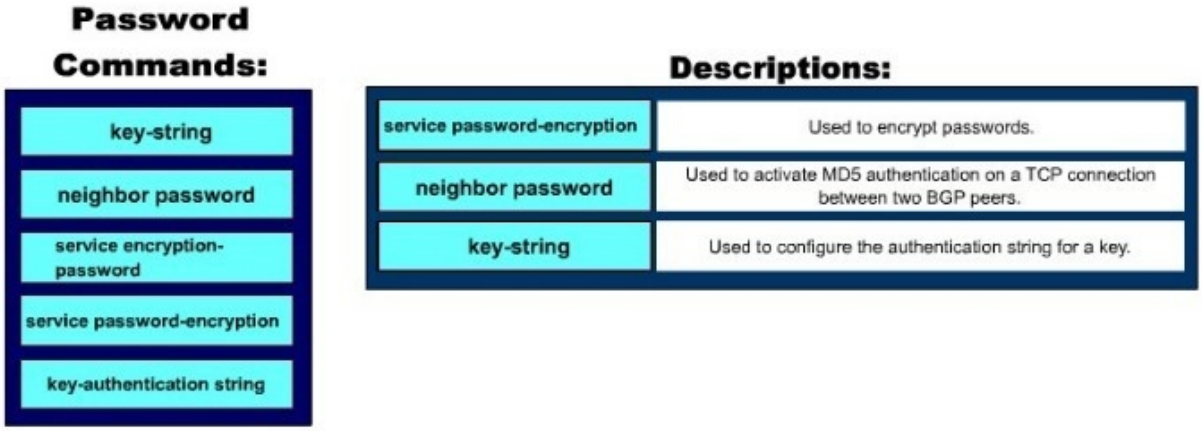
Question 150

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



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

Explanation:

Following are the commands along with their descriptions:

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

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

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

The other options offered are not valid commands.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Cisco IOS Security Command Reference > service password-encryption

Cisco > Cisco IOS IP Routing: BGP Command Reference > neighbor password

Licensed to Berend Post berend.post@it-university.nl

Question 151

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

- ☒ cell-switching
- ☐ virtual switching
- ☐ circuit-switching
- ☐ packet switching

Explanation:

Explanation:

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

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

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

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

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 152

Which Cisco IOS command will enable a switch to copy the configuration from NVRAM to its RAM?

- ☐ copy tftp flash
- ☐ copy running-config flash
- ☐ copy startup-config flash
- ☒ copy startup-config running-config
- ☐ copy running-config startup config

Explanation:

Explanation:

The copy startup-config running-config command enables a switch (or a router) to copy configuration from NVRAM to its RAM. The configuration file located in NVRAM is referred to as the startup configuration, and a configuration currently loaded and running in RAM is referred to as the running configuration.

The copy running-config startup-config command is incorrect because it will save your running configuration in RAM to the non-volatile NVRAM, which is the reverse of the scenario's requirement. This would be the required command to run if you have edited the running configuration and would like to save the changes so that they are effective the next time you restart the switch.

The copy tftp flash command does not enable a switch to copy the configuration from NVRAM to its RAM. This command is used to restore backup IOS images stored on a TFTP server to the target switch (or router).

The copy running-config flash command does not enable a switch to copy the configuration from NVRAM to its RAM. This command is used to save the running configuration in RAM to the switch's flash memory.

The copy startup-config flash command does not enable a switch to copy the configuration from NVRAM to its RAM. This command is used to save the startup configuration in NVRAM to the switch's flash memory.

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Cisco IOS Configuration Fundamentals Command Reference > C > copy

Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 8: Managing Configuration Files > Managing Configuration Files

Question 153

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

- ☐ Holddown timer
- ☐ Triggered updates
- ☐ Route poisoning
- ☒ Split horizon
- ☐ Maximum hop count

Explanation:

Explanation:

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

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

Licensed to Berend Post berend.post@it-university.nl

References:

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

Question 154

Enhanced Interior Gateway Routing Protocol (EIGRP) uses which algorithm to select the best path to the destination?

- ☒ Diffusing Update Algorithm (DUAL)
- ☐ Dijkstra algorithm
- ☐ Bellman-Ford algorithm
- ☐ Shortest Path First (SPF) algorithm

Explanation:

Explanation:

EIGRP uses the Diffusing Update Algorithm (DUAL) to select the best path to the destination. EIGRP is a classless protocol that allows the use of variable length subnet masks (VLSM), and supports classless interdomain routing (CIDR) for the allocation of IP addresses.

EIGRP is characterized by these components:

DUAL: EIGRP implements DUAL to select paths free of routing loops. DUAL selects the best path and the second best path to the destination. The terminology used in DUAL is as follows:

- Successor: Best path selected by DUAL.

- Feasible successor: Second best path selected by DUAL. This is a backup route stored in the topology table.

- Feasible distance: The lowest calculated metric of a path to destination.

Protocol-dependent modules: Different modules are used by EIGRP to independently support Internet Protocol (IP), Internetwork Packet Exchange (IPX), and AppleTalk routed protocols. These modules act as a logical interface between DUAL and routing protocols.

Neighbor discovery and recovery: Neighbors are discovered and information about neighbors is maintained by EIGRP. A hello packet is multicast on 224.0.0.10 every five seconds and the router builds a table with the information. EIGRP also enables proper operation over a Non-Broadcast Multiple Access (NBMA) point-to-multipoint network. EIGRP multicasts a hello packet every 60 seconds on the multipoint Wide Area Network (WAN) interfaces (X.25, frame relay, or Asynchronous Transfer Mode).

Reliable Transport Protocol (RTP): RTP is used by EIGRP to manage EIGRP packets. Reliable and ordered delivery of route updates is ensured using RTP.

Licensed to Berend Post berend.post@it-university.nl

EIGRP updates about routes can contain five metrics: minimum bandwidth, delay, load, reliability, and maximum transmission unit (MTU). Of these five metrics, by default, only minimum bandwidth and delay are used to compute the best path.

The Dijkstra algorithm and Shortest Path First (SPF) algorithm are used by the Open Shortest Path First (OSPF) routing protocol for selecting the best path to the destination, not by EIGRP.

The Bellman-Ford algorithm is used by Routing Information Protocol (RIP).

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast interior and exterior routing protocols

References:

Cisco > Internetworking Technology Handbook > Enhanced Interior Gateway Routing Protocol (EIGRP)

Question 155

How is load balancing achieved when implementing HSRP?

- ☐ By configuring multiple gateways on the routers
- ☒ By using multiple HSRP groups
- ☐ By configuring the same priority on all HSRP group members
- ☐ By configuring multiple virtual router addresses

Explanation:

Explanation:

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

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

Licensed to Berend Post berend.post@it-university.nl

interface fastethernet 0/1

no switchport

ip address 192.168.5.5 255.2555.255.0

standby 1 ip 192.168.5.10

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

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

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

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

Question 156

Which command is used to view the entire routing table?

- ☐ show route-map
- ☐ show ip mroute
- ☒ show ip route
- ☐ show ip protocols

Explanation:

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]]

 Licensed to Berend Post berend.post@it-university.nl

The parameters of the show ip route command are as follows:

address: Specifies the address for which the routing information should be displayed.

mask: Specifies the subnet mask.

longer-prefixes: Specifies the combination of mask and address.

protocol: Specifies the name of the routing protocols such as Routing Information Protocol (RIP), or Open Shortest Path First (OSPF).

protocol-id: Specifies the protocol ID used to identify a process of a particular protocol.

The show route-map command is incorrect because this command is used to view the route-maps configured on the router.

The show ip mroute command is incorrect because this command is used to view the contents of the IP multicast routing table.

The show ip protocols command is incorrect because this command is used to view the routing protocols parameters, and the current timer values.

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Question 157

Which is NOT a valid range for private IP addresses?

- ☐ 10.0.0.0 - 10.255.255.255
- ☐ 172.16.0.0 - 172.31.255.255
- ☐ 192.168.0.0 - 192.168.255.255
- ☒ 192.255.255.255-193.0.0.0

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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

10.0.0.0 - 10.255.255.255 (10.0.0.0/8)

172.16.0.0 - 172.31.255.255 (172.16.0.0/12)

192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

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

Objective:

Network Fundamentals

Sub-Objective:

Describe the need for private IPv4 addressing

References:

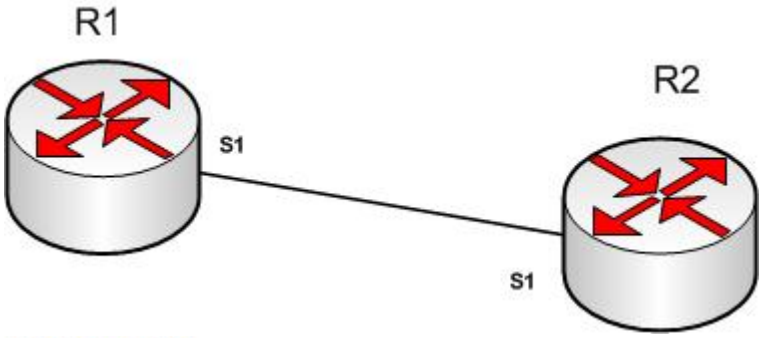
http://www.ietf.org/rfc/rfc1918.txt

http://www.iana.org/

Licensed to Berend Post berend.post@it-university.nl

Question 158

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




```
R1#show run

version 12.0
hostname R1

interface s1
ip address 192.168.5.5 255.255.255.252

ip host R1 192.168.5.6

R2#show run

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

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

- ☐ R1(config)#int S1
- ☐ R1(config-if)#no ip address 192.168.5.5
- ☐ R1(config-if)# ip address 192.168.5.9 255.255.255.252
- ☒ R1(config)#no ip host R1
- ☒ R1(config)# ip host R2 192.168.5.6 255.255.255.252
- ☐ R1(config)#no hostname R2
- ☐ R1(config)# hostname R1
- ☐ R2(config)#int S1
- ☐ R1(config-if)#no ip address 192.168.5.5
- ☐ R1(config-if)# ip address 192.168.5.9 255.255.255.0

Explanation:

Explanation:

Both routers have been configured with the ip host command. This command creates a name to IP address mapping, thereby enabling the pinging of the device by address. On R1, the mapping is incorrect and needs to be corrected. Currently it is configured as ip host R1 192.168.5.6. It is currently mapping its own name to the IP address of R2.

Licensed to Berend Post berend.post@it-university.nl

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

R1(config)#no ip host R1

R1(config)# ip host R2 192.168.5.6 255.255.255.252

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

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

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

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

Objective:

Infrastructure Services

Sub-Objective:

Troubleshoot client connectivity issues involving DNS

References:

Licensed to Berend Post berend.post@it-university.nl

Question 159

Which is the shortest possible notation of the following Internet Protocol version 6 (IPv6) address?

2001:0DB8:0000:0001:0000:0000:0000:F00D

- ☐ 2001:DB8::1::F00D
- ☒ 2001:DB8:0:1::F00D
- ☐ 2001:DB8:0:1:0:0:0:F00D
- ☐ 2001:0DB8:0:1::F00D

Explanation:

Explanation:

The shortest possible notation of the IPv6 address 2001:0DB8:0000:0001:0000:0000:0000:F00D is 2001:DB8:0:1::F00D. The address is shortened according to the following rules:

Remove leading zeros.

Remove the consecutive fields of zeros with double colon (::).

The double colon (::) can be used only once.

The option 2001:DB8::1::F00D is incorrect because the double colon (::) can be used only once in the process of shortening an IPv6 address.

The option 2001:DB8:0:1:0:0:0:F00D is incorrect because 2001:DB8:0:1:0:0:0:F00D can be further shortened to 2001:DB8:0:1::F00D.

The option 2001:0DB8:0:1::F00D is incorrect because 2001:0DB8:0:1::F00D can be further shortened to 2001:DB8:0:1::F00D.

Objective:

Network Fundamentals

Sub-Objective:

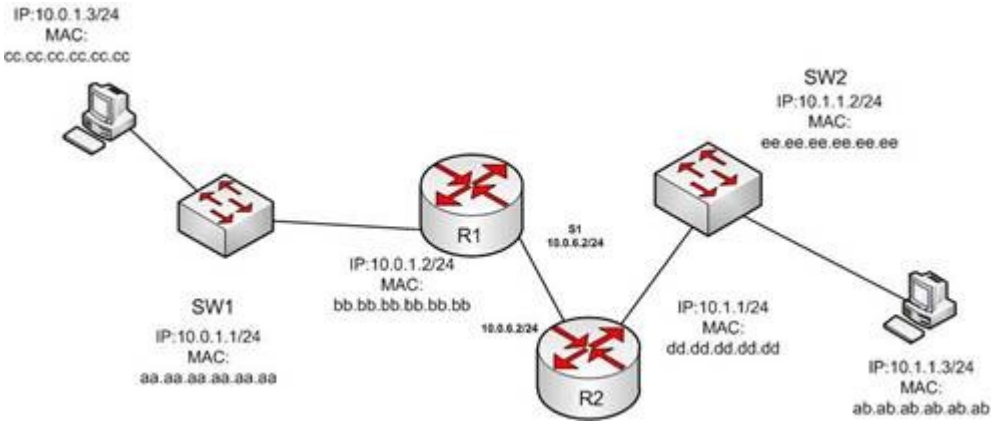
Compare and contrast IPv6 address types

References:

Licensed to Berend Post berend.post@it-university.nl

Question 160

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?



- ☐ ab.ab.ab.ab.ab.ab
- ☐ ee.ee.ee.ee.ee.ee
- ☒ dd.dd.dd.dd.dd.dd
- ☐ cc.cc.cc.cc.cc.cc
- ☐ aa.aa.aa.aa.aa.aa
- ☐ bb.bb.bb.bb.bb.bb

Explanation:

Explanation:

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Licensed to Berend Post berend.post@it-university.nl

Question 161

Examine the partial output of the show ip interface command below.

```
Router# show ip interface

Serial0 is up, line protocol is up
Internet address is 1.1.1.2/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set

GigabitEthernet0/3 is up, line protocol is up
Internet address is 192.168.93.1/28
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
```

What is the subnet broadcast address of the LAN connected to the router from which the command was executed?

- ☒ 192.168.93.15
- ☐ 192.168.93.255
- ☐ 1.1.1.255
- ☐ 1.1.1.127

Explanation:

Explanation:

In the output we can see there are two interfaces, a serial interface (which goes to another router) and a GigabitEthernet interface (the LAN interface). The LAN interface has an address of 192.168.93.1/28, which is a mask of 255.255.255.240. When this mask is used against the 192.168.93.0 classful network, it yields the following subnets:

192.168.93.0

192.168.93.16

192.168.93.32

192.168.93.48

and so on, incrementing in intervals of 16 in the last octet.

 Licensed to Berend Post berend.post@it-university.nl

Since the LAN interface has an address of 192.168.93.1, the interface is in the 192.168.93.0/28 network. That networks broadcast address is the last address before the next subnet address of 192.168.93.16. Therefore, the broadcast address of the LAN connected to the router from which the command was executed is 192.168.93.15.

The address 192.168.93.255 is not the broadcast address. If a standard 24-bit mask were used instead of the /28, this would be the broadcast address.

The address 1.1.1.255 is the broadcast address of the network in which the Serial interface resides. The question asked for the LAN interface.

The address 1.1.1.127 would be the broadcast address of the network in which the Serial interface resides if the mask used on the interface were 255.255.255.128. However, that is not the mask, and the question asked for the LAN interface.

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Question 162

What Cisco Catalyst switch feature can be used to define ports as trusted for DHCP server connections?

- ☒ DHCP snooping
- ☐ port security
- ☐ 802.1x
- ☐ private VLANs

Explanation:

Explanation:

DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP spoofing is an attack that can be used to force user traffic through an attacking device. This is accomplished by an attacker responding to DHCP queries from users. Eliminating the response from the correct DHCP server would make this more effective, but if the attacker's response gets to the client first, the client will accept it.

Licensed to Berend Post berend.post@it-university.nl

The DHCP response from the attacker will include a different gateway or DNS server address. If they define a different gateway, the user traffic will be forced to travel through a device controlled by the attacker. This will allow the attacker to capture traffic and gain company information. If the attacker changes the DNS server in the response, they can use their own DNS server to force traffic to selected hosts to go to a device they control. Again, this would allow the attacker to capture traffic and gain information.

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

The three required steps to implement DHCP snooping are:

1. Enable DHCP snooping globally with the ip dhcp snooping command:

   switch(config)# ip dhcp snooping

2. Enable DHCP snooping for a VLAN with the vlan parameter:

switch(config)# ip dhcp snooping vlan vlan #

   (for example, ip dhcp snooping 10 12 specifies snooping on VLANs 10 and 12)

3. Define an interface as a trusted DHCP port with the trust parameter:

   switch(config-if)# ip dhcp snooping trust

When specifying trusted ports, access ports on edge switches should be configured as untrusted, with the exception of any ports that may have company DHCP severs connected. Only ports where DHCP traffic is expected should be trusted. Most certainly, ports in any area of the network where attacks have been detected should be configured as untrusted.

Some additional parameters that can be used with the ip dhcp snooping command are:

switch(config)# ip dhcp snooping verify mac-address - this command enables DHCP MAC address verification.

switch(config)# ip dhcp snooping information option allow-untrusted - this command enables untrusted ports to accept incoming DHCP packets with option 82 information. DHCP option 82 is used to identify the location of a DHCP relay agent operating on a subnet remote to the DHCP server.

Licensed to Berend Post berend.post@it-university.nl

When DHCP snooping is enabled, no other relay agent-related commands are available. The disabled commands include:

ip dhcp relay information check global configuration

ip dhcp relay information policy global configuration

ip dhcp relay information trust-all global configuration

ip dhcp relay information option global configuration

ip dhcp relay information trusted interface configuration

Private VLANs are a method of protecting or isolating different devices on the same port and VLAN. A VLAN can be divided into private VLANs, where some devices are able to access other devices and some are completely isolated from others. This was designed so service providers could keep customers on the same port isolated from each other, even if the customers had the same Layer 3 networks.

Port security is a method of only permitting specified MAC addresses access to a switch port. This can be used to define what computer or device can be connected to a port, but not to limit which ports can have DHCP servers connected to them.

802.1x is a method of determining authentication before permitting access to a switch port. This is useful in restricting who can connect to the switch, but it cannot control which ports are permitted to have a DHCP server attached to it.

Objective:

Infrastructure Security

Sub-Objective:

Describe common access layer threat mitigation techniques

References:

Home > Support > Product Support > Switches > Cisco Catalyst 4500 Series Switches > Configure > Configuration Guides > Chapter: Configuring DHCP Snooping and IP Source Guard > Configuring DHCP Snooping on the Switch

Licensed to Berend Post berend.post@it-university.nl

Question 163

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

- ☒ show spanning-tree vlan vlan-id
- ☐ show vlan database
- ☐ show vlan vlan-id
- ☐ show vlan brief

Explanation:

Explanation:

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

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

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

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

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Cisco > Cisco IOS LAN Switching Command Reference, Release 12.4 > show vlan

Licensed to Berend Post berend.post@it-university.nl

Question 164

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

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

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

- ☒ the command syntax is incorrect
- ☐ the interface type does not exist on this router
- ☐ the command is entered at the wrong prompt
- ☐ the interface is configured already

Explanation:

Explanation:

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

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

```
Router78(config)#interface Serial0

%invalid input detected at '^' marker.
```

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

Licensed to Berend Post berend.post@it-university.nl

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

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

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

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

Configuration register is 0x2102
```

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Licensed to Berend Post berend.post@it-university.nl

Question 165

Which statement is supported by the following output?

router# show ip protocols
Routing Protocol is "eigrp 3"
Sending updates every 90 seconds, next due in 24 seconds
<<some output omitted>>
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 3
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
172.160.72.0
192.168.14.0
<<output omitted>>

- ☐ EIGRP supports load-balancing over three equal-cost paths
- ☐ EIGRP supports load-balancing over three unequal-cost paths
- ☒ EIGRP supports load-balancing over four equal-cost paths
- ☐ EIGRP supports load-balancing over four unequal-cost paths

Explanation:

Explanation:

The Maximum path: 4 output indicates that Enhanced Interior Gateway Routing Protocol (EIGRP) will support round-robin load-balancing over four equal-cost paths. This is a default setting, and is a true statement for most routing protocols (including RIP, OSPF and IS-IS). Equal-cost paths are different routes to the same destination network with identical metrics, as determined by the routing protocol. Most routing protocols allow this maximum to be raised up to 16 with the maximum-paths command.

EIGRP has the additional benefit of allowing unequal cost load-balancing. With unequal cost load-balancing, the router can be configured to include less desirable (higher-metric) paths in the routing table. The router will then send a balanced percentage of traffic over both the best route and the less desirable paths, such as sending two packets over the best path plus one over a less desirable path. EIGRP will never perform unequal-cost load-balancing by default; it must be configured with a variance command. Therefore, you cannot state that EIGRP supports load-balancing over unequal-cost paths in this example.

You cannot state that EIGRP will support load-balancing over three paths because the output displays the Maximum path: 4 value.

Objective:

 Licensed to Berend Post berend.post@it-university.nl

Routing Fundamentals

Sub-Objective:

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

References:

Cisco > Support > IP > IP Routing > Design > Design TechNotes > How Does Load Balancing Work? > Document ID: 5212

Cisco > Support > IP > IP Routing > Design > Design TechNotes > How Does Unequal Cost Path Load Balancing (Variance) Work in IGRP and EIGRP? > Document ID: 13677

Question 166

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

- ☐ v.35
- ☐ crossover
- ☐ rollover
- ☒ straight-through

Explanation:

Explanation:

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

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

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

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

 Licensed to Berend Post berend.post@it-university.nl

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

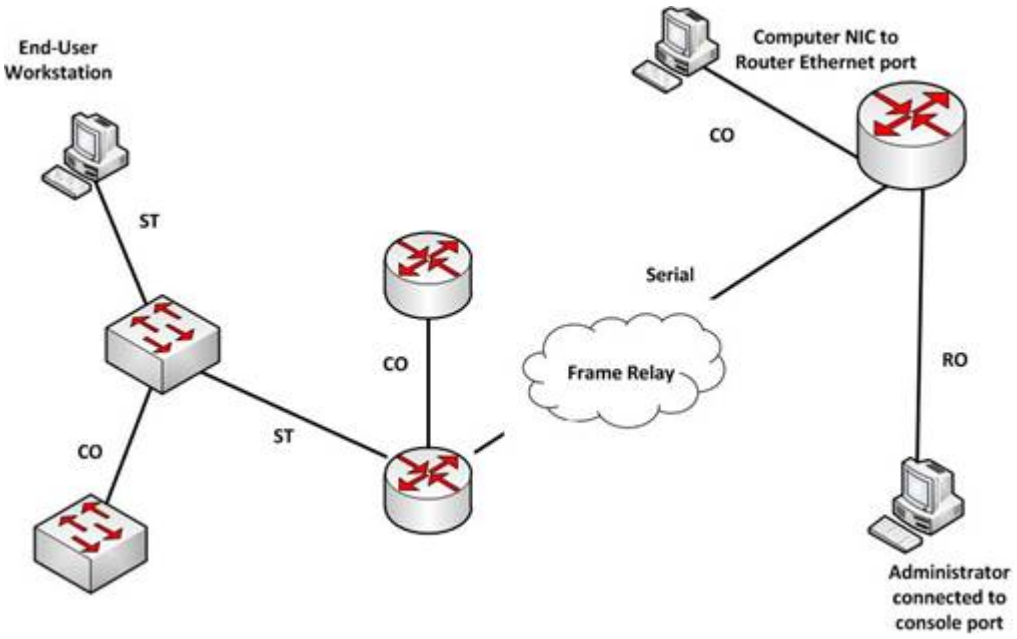
The diagram below illustrates the correct usage of each of the cable types shown using the following legend:

SO Ethernet Straight through Cable

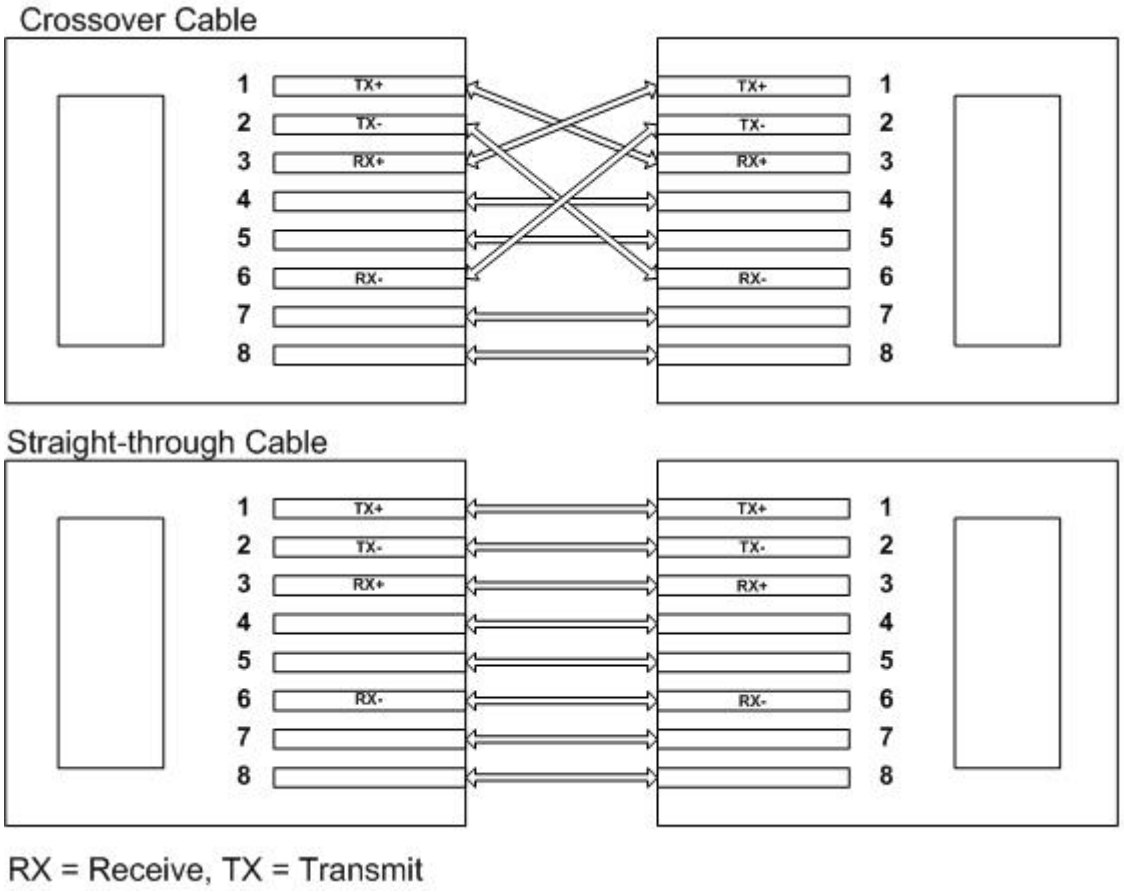
CO Ethernet Crossover Cable

Serial Serial cable

RO Rollover cable



Licensed to Berend Post berend.post@it-university.nl



RX = Receive, TX = Transmit

Objective:

Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

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

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

Licensed to Berend Post berend.post@it-university.nl

Question 167

A newly implemented IP-based video conferencing application is causing the network to slow down.

Which OSI layer needs to be addressed to resolve the problem?

- ☒ Layer 1
- ☐ Layer 2
- ☐ Layer 3
- ☐ Layer 4
- ☐ Layer 5
- ☐ Layer 6
- ☐ Layer 7

Explanation:

Explanation:

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

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

Application: Interacts directly with the application. It provides application services, such as e-mail and File Transfer Protocol (FTP).

Presentation: Enables coding and conversion functions for application layer data. The Presentation layer converts data into a format that is acceptable by the application layer. The formatting and encryption of data is done at this layer.

Session: Creates, manages, and terminates sessions between communicating nodes. The session layer handles the service requests and responses that take place between different hosts.

Transport: Delivers data sequentially and without errors. This layer manages data transmission between devices, a process known as flow control. The Transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Network: Defines the network address or the Internet Protocol (IP) address, which is then used by the routers to forward the packets.

Data Link: Ensures the reliable delivery of data to the physical address of the destination.

include fiber optic, wireless, and Ethernet.

Objective:

Licensed to Berend Post berend.post@it-university.nl

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco Documentation > Internetworking Technology Handbook > Internetworking Basics > Open System Interconnection Reference Model

Question 168

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

- ☒ PPP
- ☐ AAA
- ☐ WEP
- ☐ STP
- ☒ HDLC
- ☒ Frame Relay

Explanation:

Explanation:

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

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

Can be used over analog circuits

Can encapsulate several routed protocols, such as TCP/IP

Provides error correction

Should be used rather than HDLC when non-Cisco routers are involved, as it is implemented consistently among vendors

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

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

 Licensed to Berend Post berend.post@it-university.nl

router(config)#interface serial S0

router(config-if)#encapsulation ppp

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

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

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

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

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

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco > Internetworking Technology Handbook > Point-to-Point Protocol

Cisco > Internetworking Technology Handbook > Frame Relay

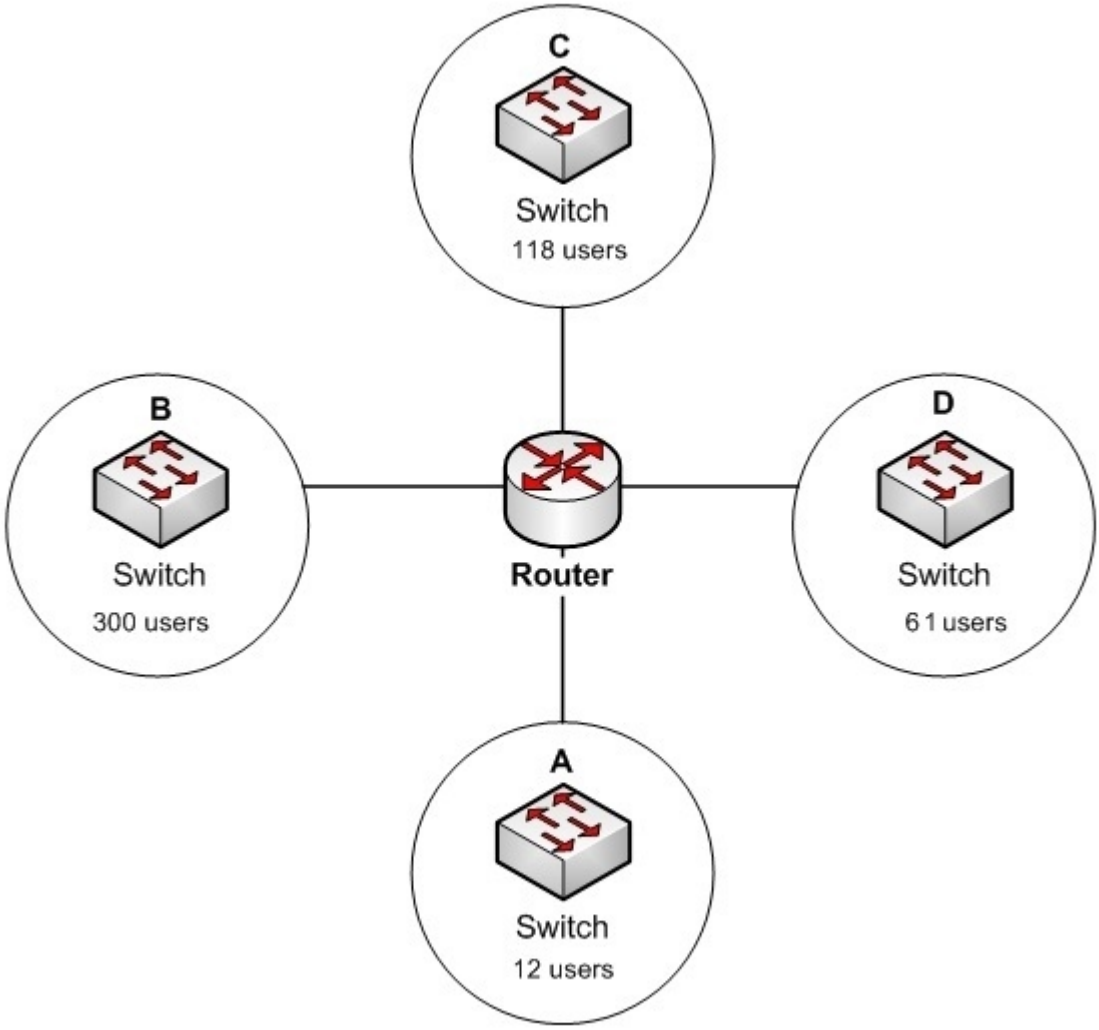
Cisco > Support > Technology Support > WAN > High-Level Data Link Control (HDLC) > Configure > Configuration Examples and TechNotes > HDLC Back-to-Back Connections > Document ID: 7927

Licensed to Berend Post berend.post@it-university.nl

Question 169

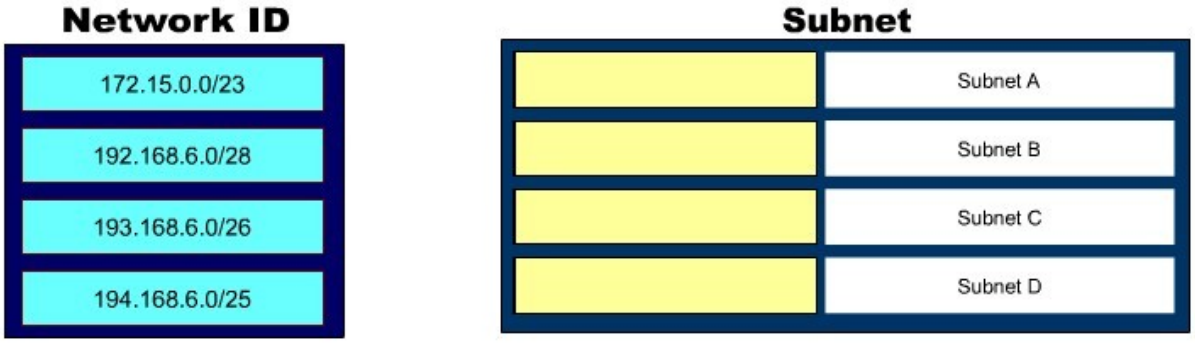
DRAG DROP

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.

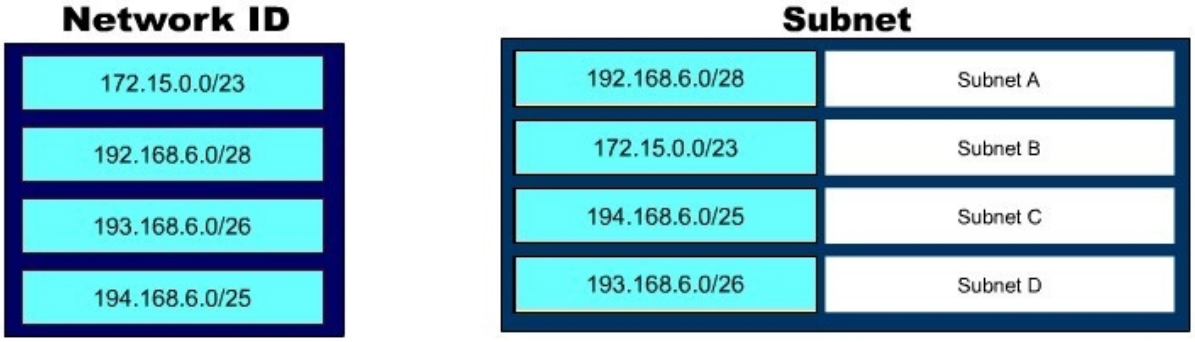


You are designing the IP addressing for this network. You are instructed not to waste IP addresses by making the subnets larger than necessary. Click and drag the correct network ID from the left to the appropriate subnet on the right.

Licensed to Berend Post berend.post@it-university.nl



Solution:



Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

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

Cisco > Technology Support > IP > IP Addressing Services > Design Technotes > Subnet Zero and the All-Ones Subnet > Document ID: 13711

Question 170

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.)

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

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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

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

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

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

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

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Cisco > Internetworking Technology Handbook > Point to Point Protocol (PPP)

Cisco > Support > Product Support > Cisco IOS Software Releases 11.1 > Configure > Feature Guides > Clock Rate Command Enhancements Feature Module > clock rate

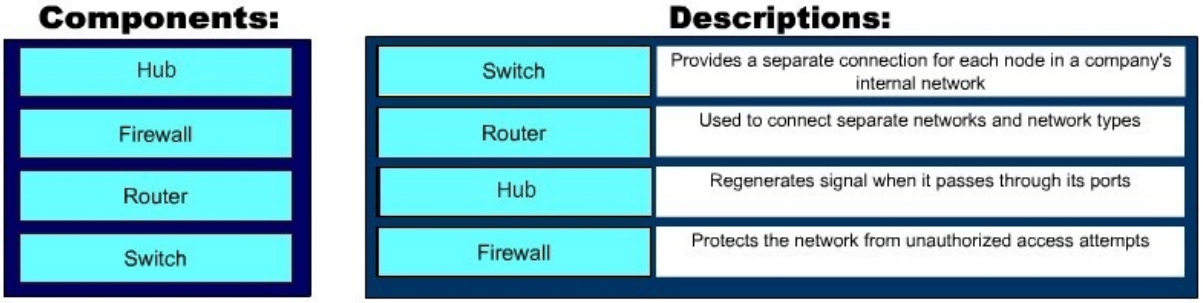
Licensed to Berend Post berend.post@it-university.nl

Question 171

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



Solution:



Explanation:

Explanation:

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

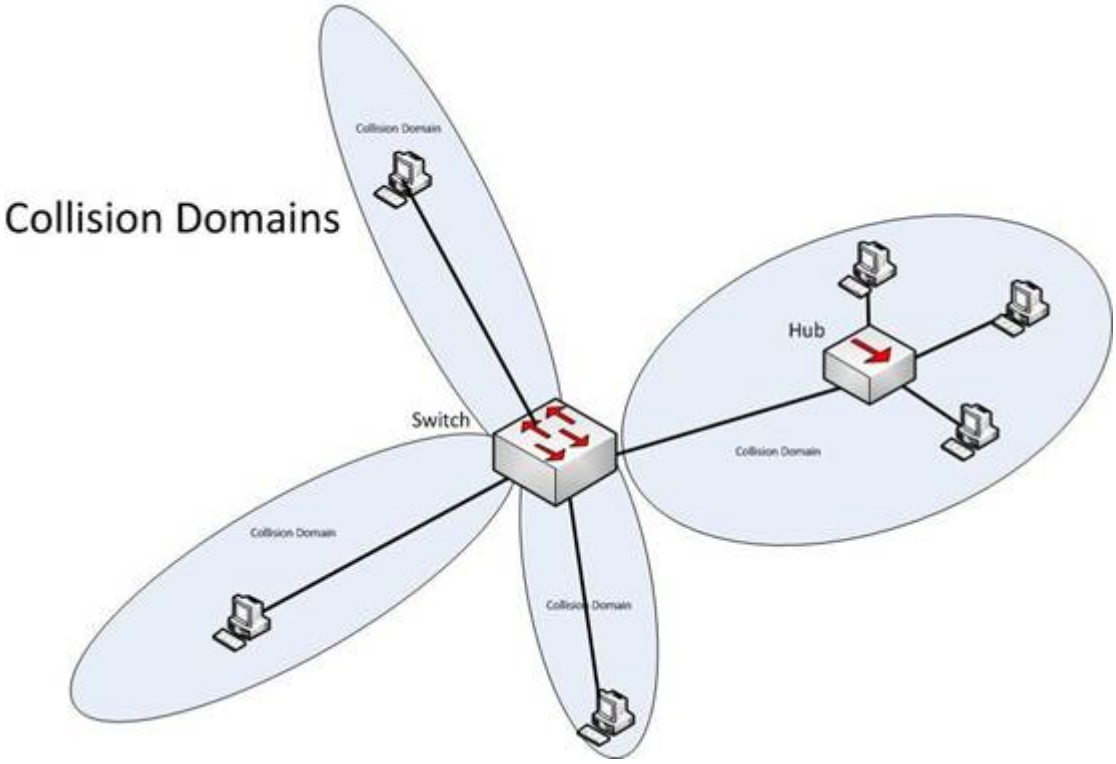
Hub: Regenerates a signal when it passes through its ports. Hubs provide a common connection point for network devices. Hubs are generally used for LAN connectivity and works at Layer 1 of the OSI model.

Firewall: Protects the network from unauthorized access attempts. It is typically placed between the Internet and a private 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.

Licensed to Berend Post berend.post@it-university.nl



Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

References:

Cisco Documentation > Internetwork Design Guide > Internetworking Design Basics

Licensed to Berend Post berend.post@it-university.nl

Question 172

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

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

What does the value 110 represent in the output?

- ☒ OSPF administrative distance
- ☐ EIGRP administrative distance
- ☐ OSPF cost
- ☐ EIGRP cost

Explanation:

Explanation:

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

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

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

The values do not represent an EIGRP cost. First, if it were an EIGRP route, the route would have a D to the left of the route details. Moreover, the cost value is located within the square brackets to the

 Licensed to Berend Post berend.post@it-university.nl

right of the forward slash in each route entry. The only cost values shown in the table are 2, 11, and 12.

Objective:

Routing Fundamentals

Sub-Objective:

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

References:

Cisco > Support > Cisco IOS IP Routing: Protocol-Independent Command Reference > show ip route

The Anatomy of "Show IP Route"

Question 173

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

- ☐ ip default-route 172.16.0.254 255.255.0.0
- ☒ ip route 0.0.0.0 0.0.0.0 172.16.0.254
- ☐ default-gateway 172.16.0.254
- ☐ ip route default 172.16.0.254

Explanation:

Explanation:

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

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

The attributes of the command are as follows:

destination_network: Defines the network that needs to be added in the routing table.

mask: Defines the subnet mask used on the network.

next-hop_address: Defines the default gateway or next-hop router that receives and forwards the packets to the remote network.

administrative_distance (AD): States the administrative distance. Static routes have an AD of 1, which can be changed to change the priority of the route.

 Licensed to Berend Post berend.post@it-university.nl

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

router(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.254

Any route configured manually is considered a static route. Another example of a command that creates a non-default route is shown below:

router(config)# ip route 192.168.12.0 255.255.255.0 172.65.3.1

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

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

router(config)# ip route 192.168.12.0 255.255.255.0 172.65.3.1 150

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

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

S*0.0.0.0/0 [1/0] via 172.16.0.254

S 192.168.12.0/24 [1/0] via 172.65.3.1

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

Licensed to Berend Post berend.post@it-university.nl

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

Cisco > Cisco ASDM User Guide, 6.1 > Configuring Dynamic And Static Routing > Field Information for Static Routes

Cisco > Support > IP > IP Routing > Design > Design TechNotes > Specifying a Next Hop IP Address for Static Routes > Document ID: 27082

Question 174

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

Which of the following statements is true of OSPFv3?

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

Explanation:

Explanation:

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

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

Router IDs should not match.

Router IDs should reflect the correct router ID for each device.

Area IDs must match.

Area types must match.

Objective:

Routing Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

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

References:

Home > Network Infrastructure > IPv6 Integration and Transition > Troubleshooting OSPFv3 Neighbor Adjacencies

Question 175

Which of the following statements best describes the result of issuing the command standby 44 timers 3 1 on an HSRP router?

- ☐ The holdtime will be set to a value of 3, and the hellotime will be set to a value of 1.
- ☐ The status of the standby router will be displayed as unknown expired.
- ☒ The role of active router will be passed repeatedly from one router to another.
- ☐ The router will be configured to reassume the role of active router in the event that the router fails and is subsequently restarted.

Explanation:

Explanation:

When the command standby 44 timers 3 1 is issued on a Hot Standby Routing Protocol (HSRP) router, the role of active router will be passed repeatedly from one router to another. This behavior occurs when the timers are set incorrectly. The syntax for the standby timers command is standby [group-number] timers [hellotime holdtime].

The hellotime variable is the number of seconds between hello messages and is set to a value of 3 by default.

The holdtime variable is the number of seconds that the HSRP standby router will wait before assuming that the active router is down; if the standby router believes the active router to be down, it will assume the role of active router.

The holdtime is set to a value of 10 by default. The holdtime should be set to a value at least three times the value of the hellotime. Otherwise, the active router might not be able to respond before the standby router assumes that the active router is down and becomes the new active router.

Because the command standby 44 timers 3 1 sets the hellotime to a value of 3 and the holdtime to a value of 1, the role of active router will be passed from one standby router to the next. To set the holdtime to a value of 3 and the hellotime to a value of 1, the command standby 44 timers 1 3 should

 Licensed to Berend Post berend.post@it-university.nl

be issued. To reset the timer values to their default values, the command no standby group-number timers should be issued.

The status of the standby router will be displayed as unknown expired if a Physical layer problem exists. The unknown expired status can also be displayed if only one HSRP router is configured for the subnet.

To configure an HSRP router to reassume the role of active router in the event that the router fails and is subsequently restarted, the command standby group-number preempt should be issued. When the HSRP active router fails or is shut down, the standby router assumes the role of active router. By default, when the original HSRP active router is restarted, it does not take the role of active router away from the original standby router, even if the original active router has a higher priority value. The command standby group-number preempt changes this default behavior.

The holdtime will not be set to a value of 3, and the hellotime will not be set to a value of 1. On the contrary, the hellotime will be set to a value of 3 and the holdtime will be set to a value of 1.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco IOS IP Application Services Command Reference > show vrrp through synguard (virtual server) > standby timers

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

Question 176

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

- ☒ Restart the router.
- ☒ Configure the enable secret password.
- ☒ Enter the router diagnostic mode.
- ☐ Enter user mode.
- ☐ Answer the security question to recover the password.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

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

Configure the router so that it starts without reading the non-volatile random access memory (NVRAM). This is also referred to as the system test mode, which you enter by changing the configuration register. You must first restart the router and within 60 seconds press Break on the terminal keyboard. Then the router will skip normal reading of the startup configuration file and will go to the ROMMON prompt (shown below this text section). At this command prompt, type confreg 0x2142 to instruct the router to boot to flash memory at the next reboot. When it does, it will ignore the startup configuration file again and will behave as if it had no configuration, as a new router would.

rommon 1> confreg 0x2142

Type reset to reboot the router.

Enter enable mode through the test system mode.

View the existing password (if it can be viewed, it may be encrypted), configure a new password, or delete the configuration.

Configure the router to start by reading the NVRAM, which is done by resetting the configuration register to its normal value. Run these commands:

Router#configure terminal

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

Router(config)#config

Router(config)#config-register 0x2102

Restart the router.

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

 Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

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

Question 177

What command disables 802.1x authentication on a port and permits traffic without authentication?

- ☐ dot1x port-control disable
- ☐ dot1x port-control force-unauthorized
- ☐ dot1x port-control auto
- ☒ dot1x port-control force-authorized

Explanation:

Explanation:

The command dot1x port-control force-authorized is used to disable 802.1x on a port and permit traffic without authentication. Dot1x ports are in one of two states, authorized or unauthorized. Authorized ports permit user traffic to flow through the port. This state usually follows successful authentication. Unauthorized ports only permit authorization traffic to flow through the port.

Usually a port begins in the unauthorized state. A user is then allowed to exchange AAA authentication traffic with the port. Once the user has been authenticated successfully, the port is changed to the authorized state and the user is permitted to use the port normally.

Normal use of 802.1x has the port configured with the dot1x port-control auto statement. This places the port in the unauthorized state until successful authentication. After successful authentication, the port is changed to the authorized state.

When 802.1x is initially configured, the default port control of the ports is force-authorized. This forces the port to be in the authorized state without successful authentication. This setting disables the need for authentication and permits all traffic.

 Licensed to Berend Post berend.post@it-university.nl

The force-unauthorized keyword configures the port as an unauthorized port regardless of authentication traffic. A port configured with this key word would not permit user traffic, not even authentication traffic.

The command dot1x port-control disable is not a valid command due to incorrect syntax.

Objective:

Infrastructure Security

Sub-Objective:

Describe device security using AAA with TACACS+ and RADIUS

References:

Cisco > Catalyst 6500 Series Release 15.0SY Software Configuration Guide > Security > IEEE 802.1X Port-Based Authentication

Cisco > Support > Cisco IOS Security Command Reference: Commands D to L > dot1x port-control

Licensed to Berend Post berend.post@it-university.nl

Question 178

Which Cisco IOS command would produce the following output?

```
Serial0/0/0 is administratively down, line protocol is down
Hardware is GT96K Serial
Internet address is 134.108.28.8, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load
1/255
Encapsulation HDLC, loopback not set,
Keepalive set (10 sec)
Last input never, output 0:00:14, output hang never
Last clearing of "show interface" counters 0:00:00
Input queue 0/40/0/0, (size/max/drops/flushes);Total output drops :81071
Qeueing strategy:FIFO
Output Queue: 0/40 (size/max)
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
145 packets output, 5084 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets, 0 restarts
<<output omitted>>
```

- ☐ show ip interface
- ☐ show ip interface brief
- ☒ show interfaces
- ☐ show interface brief

Explanation:

Explanation:

The output given in the question is produced with the show interfaces command. This command is used to view the statistics for the configured interfaces on the router. From the sample output, we can determine the following facts:

The interface has not been enabled, as indicated by the first line Serial0/0/0 is administratively down. It is not ready to for to forward packets. To enable it, the no shutdown command should be entered.

Line 3 shows that the subnet mask is 255.255.255.0.

Line 3 shows that the IP address is 134.108.28.8, a public IP address.

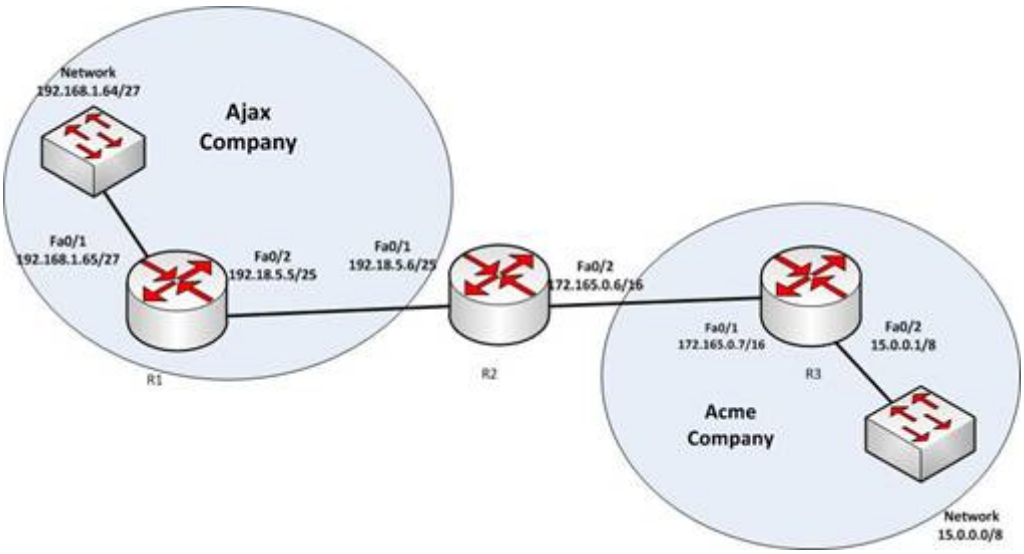
Line 6 shows that the encapsulation is HDLC, which is the default.

The interface is NOT connected to a LAN, because it is a serial interface.

Licensed to Berend Post berend.post@it-university.nl

Two fields worth mentioning in the output of the show interfaces command are the no buffer and the ignored fields. The ignored field shows the number of received packets ignored by the interface because the interface hardware ran low on internal buffers. The no buffer field shows the number of received packets discarded because there was no buffer space in the main system. When either of these two counters begins to increment, it could be the result of a broadcast storm.

Since the show interfaces command displays the up/down state of the interfaces, it is a good command for troubleshooting. For example, any time users cannot access a resource that requires them to traverse a router, it is always a good idea to use show interfaces to take a quick look at the state of the interfaces. In the example diagram below, users cannot access the resource in the network of the Acme Company from the LAN in the Ajax Company. The first step would be to execute the show interfaces command in R1 to verify functionality of the interfaces on R1.



The show ip interface command is incorrect because this command is used to view whether the interfaces configured for Internet Protocol (IP) are usable. Following is a sample output of the show ip interface command:

Licensed to Berend Post berend.post@it-university.nl

```
GigabitEthernet0/3 is up, line protocol is up
Internet address is 10.2.1.1/16
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN Flow CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is enabled, using route map PBR
Network address translation is disabled
BGP Policy Mapping is disabled
IP Multi-Processor Forwarding is enabled <======== MPF information
IP Input features, "PBR",
are not supported by MPF and are IGNORED
IP Output features, "NetFlow",
are not supported by MPF and are IGNORED
```

The show ip interface brief command is incorrect because this command provides an overview of all the interfaces configured for IP on the router. The following is sample output from the show ip interface brief command. It can be quite useful for troubleshooting as well. For example, if you cannot ping the Ethernet1 interface from a host on the Ethernet 0 LAN, you could determine from the output below that the Ethernet 1 interface is administratively down.

Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol

Ethernet0 12.17.10.5 YES NVRAM up up

Ethernet1 unassigned YES unset administratively down down

 Licensed to Berend Post berend.post@it-university.nl

Loopback0 12.17.20.5 YES NVRAM up up

Serial0 12.17.30.5 YES NVRAM up up

The solution here would be to enter configuration mode for the interface Ethernet 1 and enable it with the no shutdown command.

The show interface brief command is incorrect because this command is not a valid Cisco IOS command.

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Question 179

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

- ☒ Hello
- ☐ Update
- ☐ Queries
- ☐ Replies

Explanation:

Explanation:

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

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

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

 Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Routing Fundamentals

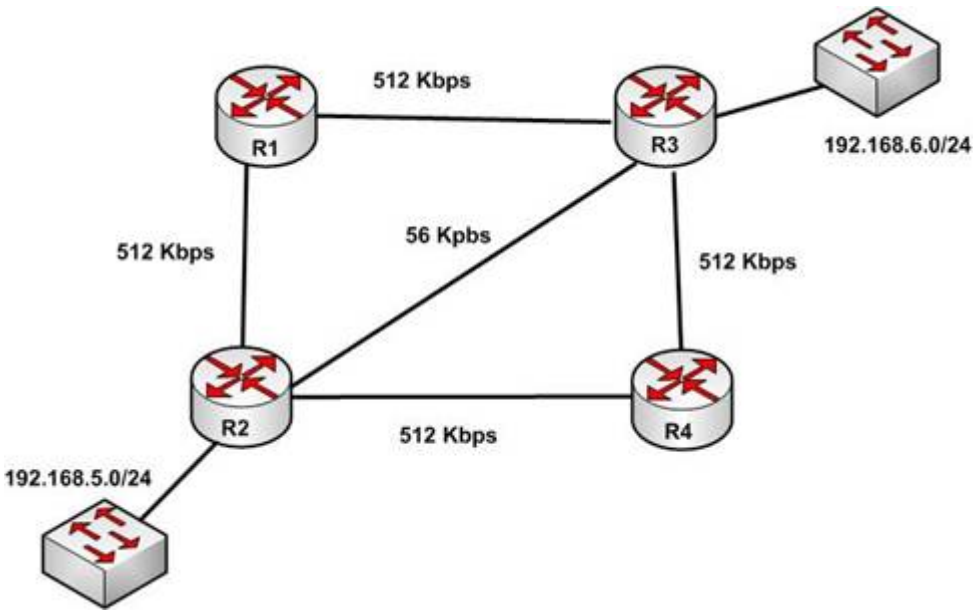
Sub-Objective:

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

References:

Question 180

With respect to the network shown below, which of the following statements are true when R2 sends a packet to the 192.168.6.0/24 network? (Choose all that apply.)



- ☐ If RIPv1 is in use, the path taken will be R2 - R4 - R3
- ☒ If both RIPv2 and EIGRP are in use, the EIGRP route will be placed in the routing table
- ☐ If EIGRP is in use, the only path taken will be R2 - R4 - R3
- ☒ If RIPv2 is in use, the path taken will be R2 - R3

Explanation:

Explanation:

If both RIPv2 and EIGRP are in use, the EIGRP route will be placed in the routing table. If RIPv2 is in use, the path taken will be R2 - R3.

Licensed to Berend Post berend.post@it-university.nl

EIGRP has a default administrative distance (AD) of 90, while RIPv2 has a default administrative distance (AD) of 120. The route learned by the routing protocol with the lowest AD will be placed in the routing table.

If you wanted to force R2 to use the RIPv2 route instead of the EIGRP route, this could be accomplished by changing the administrative distance of RIPv2 to a value less than 90, such as 80. The commands that would accomplish this are:

R2(config)# router rip

R2(config-router)# distance 80

If either of the versions of RIP is in use, hop count is used to determine the route. The path with the least number of hops is R2 - R3.

If RIPv1 is in use, the path taken would be R2 - R3, not R2 - R4 - R3, because R2 - R3 has a lower hop count.

If EIGRP is in use, the path R2 - R4 - R3 will not be the only path taken. EIGRP load-balances two equal cost paths when they exist, and R2 - R4 - R3 and R2 - R1 - R3 are of equal cost so would both be used.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

Home > Articles > Cisco Certification > CCDA > CCDA Self-Study: RIP, IGRP, and EIGRP Characteristics and Design

Licensed to Berend Post berend.post@it-university.nl

Question 181

You manage the EIGRP subnet in your organization. You have enabled EIGRP for IPv6 on all the routers in the EIGRP AS 260 using the following commands on all the routers:

The **ipv6 unicast-routing** command in global configuration mode
The **interface** command in global configuration mode
The **ipv6 enable** command in interface configuration mode
The **ipv6 eigrp** command in interface configuration mode
The **ipv6 router eigrp** command in global configuration mode
The **eigrp router-id** command in global configuration mode

During verification, you discover that EIGRP for IPv6 is not running on the routers.

Which of the following should be done to fix the issue?

- ☐ The ipv6 address command should be executed in interface configuration mode.
- ☐ The ipv6 address command should be executed in router configuration mode.
- ☐ The eigrp router-id command should be executed in interface configuration mode.
- ☒ The eigrp router-id command should be executed in router configuration mode.

Explanation:

Explanation:

The eigrp router-id command should be executed in router configuration mode to fix the issue. This command specifies a fixed router IPv4 address to the router. If this command is missing or incorrectly configured on the router, EIGRP for IPv6 will not run properly.

Another command that you should perform so that EIGRP for IPv6 runs on the routers is the no shutdown command. You should execute this command in interface configuration mode. The no shutdown command is necessary because all the interfaces with EIGRP for IPv6 enabled on them are in a shutdown state by default.

A sample configuration to implement EIGRP for IPv6 on a router is as follows:

```
Rtr63(config)# ipv6 unicast-routing
Rtr63(config) # interface Fa0/1
Rtr63(config-if) # ipv6 enable
Rtr63(config-if) # ipv6 eigrp 260
Rtr63(config-if)# no shutdown
Rtr63(config-if) # exit
Rtr63(config)# ipv6 router eigrp 260
Rtr63(config-rtr)# eigrp router-id 1.1.1.1
```

The two options stating that the ipv6 address command should be executed on the routers are incorrect. EIGRP for IPv6 can be configured on router interfaces without explicitly specifying a global unicast IPv6 address. If you specify the ipv6 enable command, as in this scenario, then the IPv6 address command is not required.

Licensed to Berend Post berend.post@it-university.nl

The option stating that the eigrp router-id command should be executed in interface configuration mode is incorrect. This command should be executed in router configuration mode instead of interface or global configuration modes.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

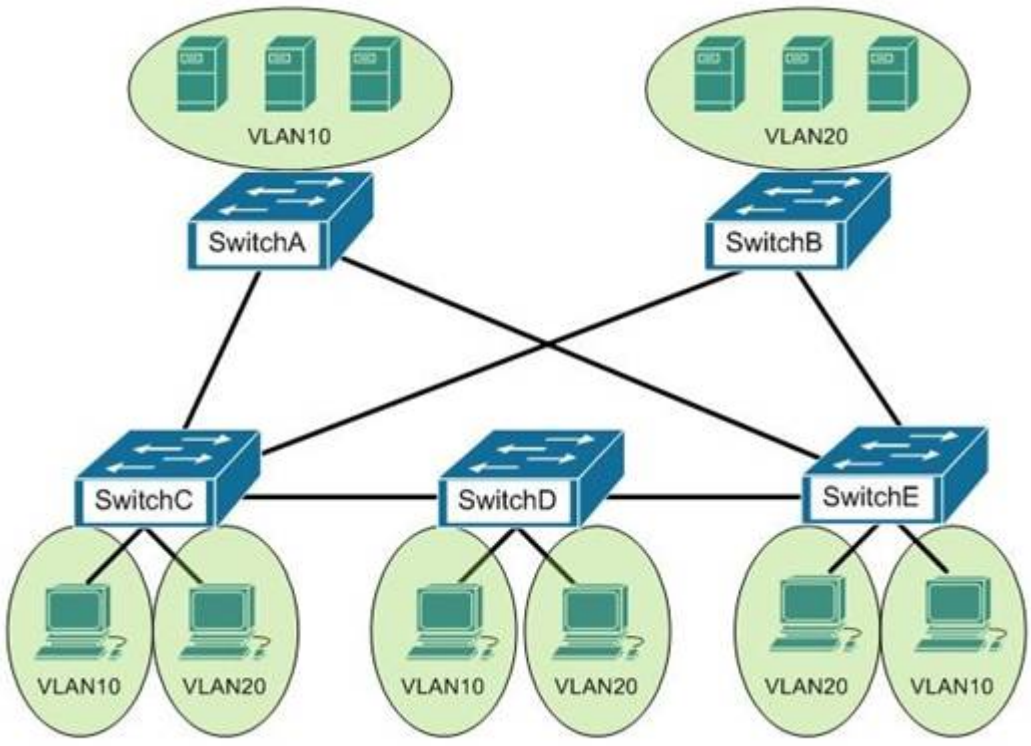
References:

Cisco IPv6 Implementation Guide, Release 15.2M&T > Implementing EIGRP for IPv6 > How to Implement EIGRP for IPv6 > Enabling EIGRP for IPv6 on an Interface

Licensed to Berend Post berend.post@it-university.nl

Question 182

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



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

- ☐ Switch A for VLAN 10 and Switch E for VLAN 20
- ☒ Switch A for VLAN 10 and Switch B for VLAN 20
- ☐ Switch A for VLAN 10 and Switch C for VLAN 20
- ☐ Switch D for VLAN 10 and Switch B for VLAN 20
- ☐ Switch E for VLAN 10 and Switch A for VLAN 20
- ☐ Switch B for VLAN 10 and Switch E for VLAN 20

Explanation:

Explanation:

You should designate Switch A for VLAN 10 and Switch B for VLAN 20. The STP root bridge for a particular VLAN should be placed as close as possible to the center of the VLAN. If the majority of network traffic is between the hosts and servers within each VLAN, and the servers are grouped into a server farm, then the switch that all hosts will be sending their data to is the ideal choice for the STP root. Cisco's default implementation of STP is called Per-VLAN Spanning Tree (or PVST), which allows individual tuning of the spanning tree within each VLAN. Switch A can be configured as the root bridge for VLAN 10, and Switch B can be configured as the root bridge for VLAN 20, resulting in optimized traffic flow for both.

Licensed to Berend Post berend.post@it-university.nl

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

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

Question 183

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

- ☐ bridges
- ☒ VLANs
- ☐ switches
- ☐ hubs

Explanation:

Explanation:

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

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

A hub does not split the network into separate broadcast domains. A hub regenerates signal when it passes through its ports, which means that it acts as a repeater and port concentrator only. Hubs and repeaters are Layer 1 devices that can be used to enlarge the area covered by a single LAN segment,

 Licensed to Berend Post berend.post@it-university.nl

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

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

References:

Cisco Documentation > Internetworking Case Studies > LAN Switching

Question 184

Which of the following is NOT a characteristic of Open Shortest Path First (OSPF)?

- ☒ Is a Cisco-proprietary routing protocol
- ☐ Has a default administrative distance of 110
- ☐ Supports authentication
- ☐ Uses cost as the default metric

Explanation:

Explanation:

OSPF is not a Cisco-proprietary routing protocol. It is an industry standard protocol supported by a wide range of vendors. The following are characteristics of OSPF:

Uses Internet Protocol (IP) protocol 89.

Has a default administrative distance of 110.

Is an industry standard protocol (non Cisco-proprietary).

Supports Non-Broadcast Multi-Access (NBMA) networks such as frame relay, X.25, and Asynchronous Transfer Mode (ATM). The default hello interval for NBMA networks is 30 seconds.

Supports point-to-point and point-to-multipoint connections.

Supports authentication.

Uses 224.0.0.6 as multicast address for ALLDRouters.

Uses 224.0.0.5 as multicast address for ALLSPFRouters.

Uses link-state updates and SPF calculation that provides fast convergence.

 Licensed to Berend Post berend.post@it-university.nl

Recommended for large networks due to good scalability.

Uses cost as the default metric.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast interior and exterior routing protocols

References:

Cisco > Articles > Cisco Certification > CCNP > Shooting Trouble with IP

Cisco > Internetworking Technology Handbook > Open Shortest Path First (OSPF)

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 9: OSPF, pp. 347-361.

Question 185

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

- ☒ copy tftp flash
- ☐ copy flash tftp
- ☐ copy running-config tftp
- ☐ copy running-config startup-config
- ☐ copy tftp running-config

Explanation:

Explanation:

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

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

Verify the connectivity between Router A and Router B using the ping command.

Check the image size on both of the routers with the show flash command to verify that enough space exists on Router B.

Configure Router A as the TFTP server using the configure terminal command. Use the tftp-server flash [partition-number:]filename1 [alias filename2] [access-list-number] command to define the path to system image that needs to transferred. There can be multiple entries for multiple images.

Copy the image from Router A to Router B using the copy tftp flash command.

 Licensed to Berend Post berend.post@it-university.nl

Verify the flash for the copied new image on Router B with the show flash command.

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

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

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

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

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

Question 186

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?

- ☒ The reported stratum of the time source is 12
- ☐ The IP address configured for the time source is incorrect
- ☐ NTP authentication is failing
- ☐ There is an access list that blocks port 123

Explanation:

Explanation:

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

 Licensed to Berend Post berend.post@it-university.nl

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

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

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

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

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify NTP operating in a client/server mode

References:

Cisco > Support > Product Support > Switches > Cisco Nexus 6000 Series Switches > Configure > Configuration Guides > Cisco Nexus 6000 Series NX-OS System Management Configuration Guide, Release 7.x > Chapter: Configuring NTP

Question 187

Which Cisco Internetwork Operating System (IOS) command is used to encrypt passwords on Cisco routers?

- ☐ password secure
- ☐ service encryption-password
- ☒ service password-encryption
- ☐ enable password

Explanation:

Explanation:

The service password-encryption command is used to encrypt passwords on Cisco routers. It is used to encrypt all passwords configured on the router, both current and future. This means all passwords in the plain text configuration file will be encrypted. This command is issued in global configuration mode. The syntax of the command is as follows:

 Licensed to Berend Post berend.post@it-university.nl

Router(config)# service password-encryption

This command does not have any parameters.

Once executed any password in the configuration file will appear similar to what is shown below when the running or startup configuration files are viewed:

R1#show run

<output omitted>

line console 0

password 7 09-4f60C0B1C1B

login

<output omitted>

The password secure and service encryption-password commands are incorrect because they are not valid Cisco IOS commands.

The enable password command is used to set the privileged EXEC mode password, and does not encrypt the password by default.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Cisco IOS Security Configuration Guide, Release 12.4 > Part 7: Secure Infrastructure > Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Licensed to Berend Post berend.post@it-university.nl

Question 188

Why is it recommended to use Spanning Tree Protocol (STP) in Local Area Networks (LANs) with redundant paths?

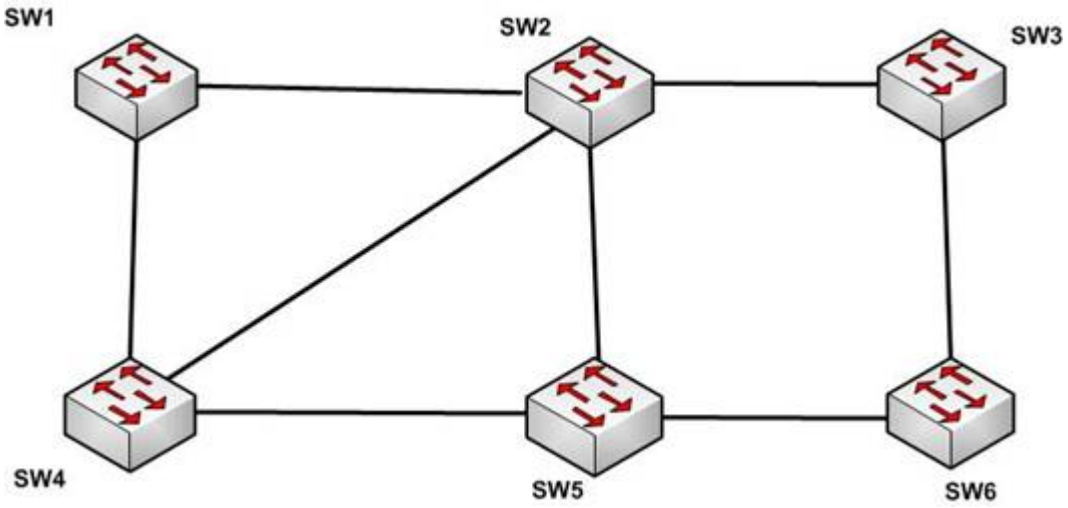
- ☒ To prevent loops
- ☐ To manage VLANs
- ☐ To load balance across different paths
- ☐ To prevent forwarding of unnecessary broadcast traffic on trunk links

Explanation:

Explanation:

Spanning Tree Protocol (STP) is a Layer 2 protocol used in LANs to maintain a loop-free network topology by recognizing physical redundancy in the network and logically blocking one or more redundant ports.

An example of switch redundancy is shown in the diagram below. The connection from SW4 to SW2, while providing beneficial redundancy, introduces the possibility of a switching loop.



STP probes the network at regular intervals to identify the failure or addition of a link, switch, or bridge. In the case of any topology changes, STP reconfigures switch ports to prevent loops. The end result is one active Layer 2 path through the switch network.

STP is not used for management of Virtual Local Area Networks (VLANs). VLAN Trunking Protocol (VTP) simplifies the management of VLANs by propagating configuration information throughout the switching fabric whenever changes are made. In the absence of VTP, switch VLAN information would have to be configured manually.

Licensed to Berend Post berend.post@it-university.nl

STP is not used to load-balance traffic across different redundant paths available in a topology. Load balancing allows a router to use multiple paths to a destination network. Routing protocols, Routing Information Protocol (RIP), RIPv2, Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Open Shortest Path First (OSPF) support load balancing. Similarly, multiple links can be combined in a faster single link in switches. This can be achieved with the Fast EtherChannel or Gigabit EtherChannel features of Cisco switches.

STP does not prevent forwarding of unnecessary broadcast traffic on trunk links. This is achieved by manually configuring VLANs allowed on the trunk, or through VTP pruning.

Objective:

LAN Switching Fundamentals

Sub-Objective:

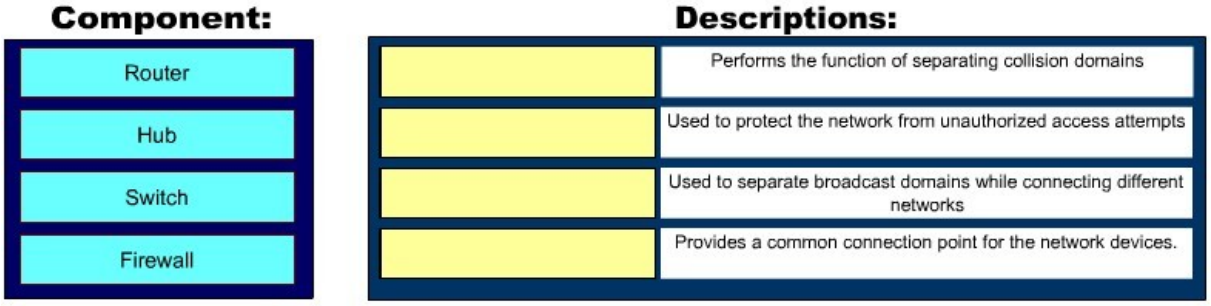
Configure, verify, and troubleshoot STP protocols

References:

Cisco > Support > Configuring Spanning Tree-Protocol > How STP Works

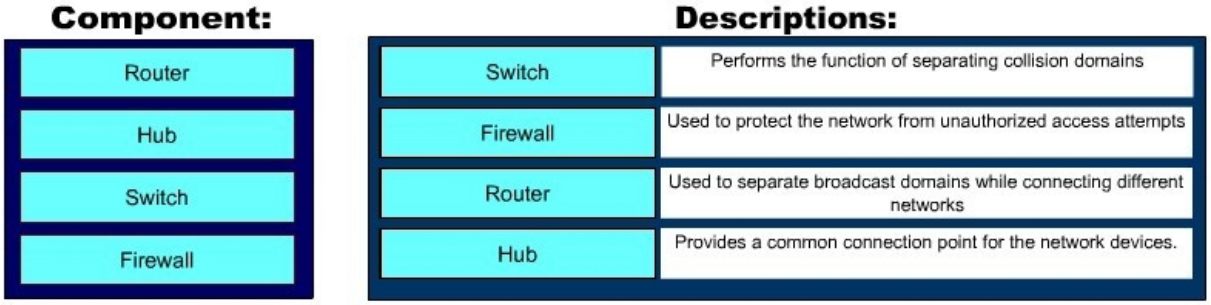
Question 189

DRAG DROP
Click and drag the components on the left to their appropriate descriptions on the right.



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

Explanation:

The following are the components used for network and Internet communications and their appropriate descriptions:

Router: Separates broadcast domains while connecting different networks. Routers provide a medium for connecting Local Area Network (LAN) and Wide Area Networks (WAN) segments

Hub: Provides a common connection point for the network devices. Hubs are generally used for LAN segmentation. A hub also regenerates the signal when it passes through its ports. Hub works at Layer 1 of the Open system Interconnection (OSI) model.

Switch: Used to provide a separate connection for each node in a company's internal network. Switches work at Layer 2 in the OSI model and perform the function of separating collision domains.

Firewall: Used to secure the network against unauthorized and malicious access attempts.

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

Reference:

Cisco > Home > Internetworking Technology Handbook > Internetworking Basics> Bridging and Switching Basics

Licensed to Berend Post berend.post@it-university.nl

Question 190

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

- ☒ An IPv6 address is divided into eight 16-bit groups.
- ☒ A double colon (::) can only be used once in a single IPv6 address.
- ☐ IPv6 addresses are 196 bits in length.
- ☐ Leading zeros cannot be omitted in an IPv6 address.
- ☒ Groups with a value of 0 can be represented with a single 0 in IPv6 address.

Explanation:

Explanation:

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

The following statements are also true regarding IPv6 address:

IPv6 addresses are 128 bits in length.

Eight 16-bit groups are divided by a colon (:).

Multiple consecutive groups of 16-bit 0s can be represented with double colon (::) (only once)

Double colons (::) represent only 0s.

Leading zeros can be omitted in an IPv6 address.

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

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

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast IPv6 address types

References:

Cisco > Cisco IOS IPv6 Configuration Guide, Release 12.4 > Implementing IPv6 Addressing and Basic Connectivity > IPv6 Address Formats

Cisco > Internetworking Technology Handbook > IPv6

 Licensed to Berend Post berend.post@it-university.nl

Question 191

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

- ☐ host to host
- ☒ switch to router
- ☐ switch to switch
- ☐ host to router's Ethernet port

Explanation:

Explanation:

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

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

Host to host Crossover

Host NIC to router Crossover

Host to switch Straight through

Switch to Switch Crossover

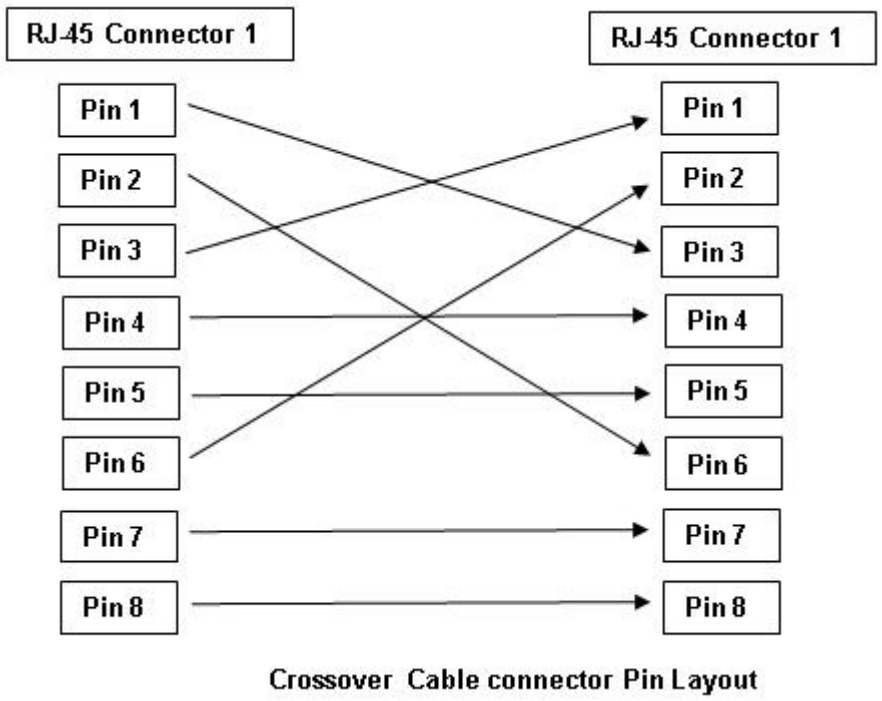
Switch to router Straight through

The difference between straight-through and crossover lies in the location of the wire termination on the two ends of an RJ-45 cable. If the unshielded twisted-pair (UTP) cable wire connects Pin 1 of one side to Pin 1 of other side and Pin 2 to 2 through all eight Pins of the RJ-45 connector, the cable is said to be straight-through.

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

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

Licensed to Berend Post berend.post@it-university.nl



Crossover Cable connector Pin Layout

Objective:

Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

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

Question 192

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

- ☐ LCP
- ☐ NCP
- ☐ PAP
- ☒ CHAP

Explanation:

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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

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

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

Authentication method used (PAP or CHAP), if any

Compression algorithm used (Stacker or Predictor), if any

Callback phone number to use, if defined

Multilink; other physical connections to use, if configured

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

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

Objective:

WAN Technologies

Sub-Objective:

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

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Internetworking Technology Handbook > Point-to-Point Protocol

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

Question 193

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

Routing Protocol	Cost
RIP	5
OSPF	25
EIGRP	2269571

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

- ☐ the RIP route
- ☐ the OSPF route
- ☒ the EIGRP route
- ☐ all of the routes

Explanation:

Explanation:

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

It selects the route with the lowest administrative distance.

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

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

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

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

Objective:

Routing Fundamentals

Sub-Objective:

 Licensed to Berend Post berend.post@it-university.nl

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

References:

Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > Route Selection in Cisco Routers

Question 194

Which of the following statements are NOT part of the guidelines for configuring VLAN Trunking Protocol (VTP) to ensure that VLAN information is distributed to all Cisco switches in the network? (Choose all that apply.)

- ☐ The VTP version must be the same on all switches in a VTP domain.
- ☒ The configuration revision number must be configured identically on all switches in a VTP domain.
- ☐ The VTP password must be the same on all switches in a VTP domain.
- ☐ The VTP domain name must be the same on all switches in a VTP domain.
- ☒ VLANs configured on clients should exist on the server switch.
- ☐ The switch(s) that will share VLAN information is(are) operating in VTP server mode
- ☐ The switches must be configured to use the same method of VLAN tagging
- ☐ The switches must be connected with trunk links

Explanation:

Explanation:

For all switches in a VTP domain, the VTP version, VTP password, and VTP domain name must be the same. Moreover, switches that will share VLAN information must be operating in VTP server mode, must be using the same VLAN tagging method (either 802.1q or ISL), and must be connected with trunk links.

Many of these settings can be verified by using the show vtp status command. By viewing the output of the command on two switches that are not sharing information, inconsistencies that prevent the sharing of VLAN information can be identified. Consider the output from the two switches below:

Licensed to Berend Post berend.post@it-university.nl

```
Switch60# show vtp status
VTP Version : 2
Configuration Revision : 62
Max VLAN support locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Server
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
```

```
Switch62# show vtp status
VTP Version : 2
Configuration Revision : 62
Max VLANs support locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Client
VTP Domain Name : Corp
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
```

```
Switch61# show vtp status
VTP Version : 2
Configuration Revision : 62
Max VLAN support locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Transparent
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
```

```
Switch63# show vtp status
VTP Version : 2
Configuration Revision : 63
Max VLAN support locally : 1005
Number of existing VLANs : 24
VTP Operating Mode : Client
VTP Domain Name : Corporate
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
```

Based on the output for the four switches, you should NOT expect Switch62 to exchange VLAN information with the other switches because the VTP domain names do not match. Line 6 shows that Swicth62 is set to Corp and the others are set to Corporate. The command to set the VTP domain name is:

Switch62(config)#vtp domain corporate

Switch62 is operating in Client mode, which means it will accept VLAN changes sent by switches operating in Server mode once the domain name mismatch is corrected. It will both process them and forward them, but will not allow VLAN changes to be made locally, and it will not save any of the VLAN information in NVRAM (line 5). The command to place a switch into Client mode is:

Switch62(config)#vtp mode client

Switch60 is operating in Server mode and will allow changes to be made locally, will send those changes to other switches, and WILL save all changes (both learned and made locally) in NVRAM, as shown by line 5. The command to place a switch into Server mode is:

Switch62(config)#vtp mode server

Switch61 is operating in Transparent mode. It will allow changes to be made locally and WILL save all changes made locally in NVRAM, but will NOT send those changes to other switches, as shown in line

Licensed to Berend Post berend.post@it-university.nl

5. It will accept and pass along VTP changes from switches operating in Server mode, but will not save those changes in NVRAM. The command to place a switch in Transparent mode is:

Switch62(config)#vtp mode transparent

Switch63 will ignore any information it receives from the other switches, even though the domain name matches, because it has a higher configuration revision number (63) than the other switches. These revision numbers are used by the switches to prevent unnecessary processing of changes that have already been received.

VTP is used to synchronize Virtual Local Area Network (VLAN) databases across switches. VTP server switches can be used to add, delete, or rename VLANs, which are then synchronized over the network with VTP client switches. This allows a network administrator to create a VLAN once, as opposed to having to create it individually on every switch on the network. The password is used to validate the source of the VTP advertisements sent between the switches in the VTP domain.

The option stating that the configuration revision number must be configured identically on all switches in a VTP domain is incorrect. The configuration number cannot be directly configured, but is instead synchronized during VTP updates.

The option stating that VLANs configured on clients should exist on the server switch is incorrect. VTP clients do not allow local VLAN configuration, and can only receive VLANs via VTP synchronization over the network.

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

Licensed to Berend Post berend.post@it-university.nl

Question 195

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

- ☒ DHCP relay agent
- ☐ DHCP BOOTP agent
- ☐ DHCP relay protocol
- ☐ DHCP BOOTP relay

Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl

The client device broadcasts a DHCPDISCOVER broadcast message to locate a DHCP server.

The DHCP server replies with a DHCPOFFER unicast message containing configuration parameters, such as an IP address, a MAC address, a domain name, and a lease for the IP address for the client device.

The client sends back a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the DHCP server.

The DHCP server replies back to client device with DHCPACK unicast message, acknowledging the allocation of the IP address to this client device.

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

All other options are invalid devices or features.

Objective:

Infrastructure Services

Sub-Objective:

Troubleshoot client- and router-based DHCP connectivity issues

References:

Cisco > Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 > Part 3: DHCP > Configuring the Cisco IOS DHCP Relay Agent

Cisco > Cisco IOS IP Application Services Command Reference > ip helper-address

Question 196

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?

- ☒ Straight-through cable
- ☐ Rollover cable
- ☐ Crossover cable
- ☐ Serial cable

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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

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

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

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

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

Objective:

LAN Switching Fundamentals

Sub-Objective:

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

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 197

Which of the following protocols is responsible for negotiating upper-layer protocols that will be carried across a Point-to-Point Protocol (PPP) connection?

- ☐ LCP
- ☒ NCP
- ☐ LMI
- ☐ ISDN

Explanation:

Explanation:

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

Link Control protocol (LCP) is not responsible for negotiating upper-layer protocols that will be carried across a PPP connection. Link Control protocol (LCP) has the primary responsibility of negotiating and maintaining the PPP connection. LCP, defined in Request for Comments (RFCs) 1548 and 1570, has the primary responsibility to establish, configure, authenticate, and test a PPP connection. LCP negotiates the following when setting up a PPP connection:

Authentication method used (PAP or CHAP), if any

Compression algorithm used (Stacker or Predictor), if any

Callback phone number to use, if defined

Multilink; other physical connections to use, if configured

Local Management Interface (LMI) is not responsible for negotiating upper-layer protocols that will be carried across the PPP connection. LMI is a characteristic of a frame relay connection. There are three types of LMIs supported by Cisco routers:

Cisco

ANSI Annex D

Q933-A Annex A

LMI has nothing to do with PPP connections.

Integrated Services Digital Network (ISDN) is a type of WAN connection and has nothing to do with PPP connections.

Objective:

Licensed to Berend Post berend.post@it-university.nl

WAN Technologies

Sub-Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

Cisco > Internetworking Technology Handbook > Point-to-Point Protocol

Cisco > Support > Technology Support > WAN > Point-to-Point Protocol (PPP) > Design > Design Technotes > Understanding and Configuring PPP CHAP Authentication > Document ID: 25647

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 12: Point-to-Point WANs, pp. 436-441.

Question 198

Which statement is TRUE of the CSMA/CD Ethernet media access method?

- ☐ It requires centralized monitoring and control.
- ☐ It is ideal for a switched network environment.
- ☒ It uses a back-off algorithm to calculate a random time value.
- ☐ Each station is allotted a time slot in which they can transmit data.

Explanation:

Explanation:

The Carrier Sense Multiple Access - Collision Detection (CSMA/CD) Ethernet Media Access Control (MAC) method uses a back-off algorithm to calculate random times to transmit packets across a channel. When two stations start transmitting at same time, their signals will collide. The CSMA/CD method detects the collision and causes both stations to hold the retransmission for an amount of time determined by the back-off algorithm. This is done in an effort to ensure that the retransmitted frames do not collide.

CSMA/CD does not require centralized monitoring and control nor does it assign time slots to stations. Moreover, the CSMA/CD method is designed to work in non-switched environment. It is an alternative to a token-passing topology, in which each station waits in turn to receive a token that allows it to transmit data. With CSMA/CD, each station is capable of making the decision regarding when to transmit the data.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco Documentation > Internetworking Technology Handbook > Ethernet Technologies

Question 199

You network team is exploring the use of switch stacking.

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

- ☒ The master switch is the only switch with full access to the interconnect bandwidth
- ☐ Switches are connected with special cable
- ☐ The stack has a single IP address
- ☐ Up to nine switches can be added to the stack

Explanation:

Explanation:

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

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

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

Up to nine switches can be in a stack.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe the benefits of switch stacking and chassis aggregation

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 200

You are configuring a Cisco router.

Which command would you use to convey a message regarding the remote access security policy of your organization to a user logging into the router?

- ☐ hostname
- ☒ banner motd
- ☐ description
- ☐ boot system
- ☐ terminal monitor

Explanation:

Explanation:

The banner motd command is used to specify a message of the day (MOTD) banner to users logging into the router. This is a global configuration mode command and is generally used to communicate routers identification information, display any warning specific to the router, or display a remote access security policy, such as "Unauthorized access to the router is prohibited." The syntax for this command is as follows:

banner motd [d message d]

d is the delimiter character. It can be any character of the administrator's choice, with the limitation that the delimiter character cannot be used in the message text.

The hostname command is a global configuration command to assign the router a name for identification. The command syntax is hostname [name].

The description command is an interface configuration mode command that sets a description for that interface.

The boot system command is used to specify the path to the primary IOS file. It is a global configuration command.

The terminal monitor command is used to direct debug and system error message to the monitor when connected to a router using telnet. When you are connected to a router using telnet and you issue the debug command, by default the output can only have been seen through a console session with that router. Executing the terminal monitor command directs that output to the terminal session where it can be viewed.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Cisco IOS Configuration Fundamentals Command Reference > F through K > banner motd

Question 201

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

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

- ☐ it uses the existing cable TV connection
- ☒ it uses the existing phone line
- ☐ you receive a committed information rate (CIR) from the provider
- ☐ the upload rate is as good as the download rate

Explanation:

Explanation:

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

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

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

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

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

Licensed to Berend Post berend.post@it-university.nl

References:

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

Question 202

Which Cisco Internetwork Operating System (IOS) command is used to make the running configuration in Random Access Memory (RAM) to the configuration the router will use at startup?

- ☒ copy running-config startup-config
- ☐ copy flash running-config
- ☐ copy tftp flash
- ☐ copy running-config flash memory
- ☐ copy startup-config tftp
- ☐ copy tftp running-config
- ☐ copy running-config tftp

Explanation:

Explanation:

The copy running-config startup-config command is used to make the running configuration in Random Access Memory (RAM) the configuration the router will use at startup. It saves the running configuration in RAM to the router's NVRAM. This command should always follow changes to the configuration; otherwise, the changes will be lost at the next router restart. The startup configuration loads into memory from NVRAM at boot and resides in memory. When the router restarts, memory information is lost.

The copy flash running-config command is incorrect because this would copy a configuration from the router's flash memory to the running configuration, causing it to be the active configuration. While this can be done, it is not a common practice. Configuration files are normally stored in NVRAM.

The copy tftp flash command is incorrect because this command is used to replace the IOS image with a backup IOS image stored on a TFTP server to the target router. A router can also act as a TFTP server for another router. When you execute this command, you will be prompted for the IP address or hostname of the TFTP server. This prompt will display as in this example:

router#enable

router#copy tftp flash

Address or name of remote host []? 192.168.1.5.2

 Licensed to Berend Post berend.post@it-university.nl

Before performing an upgrade of the IOS version from a TFTP server, you should verify that the upgrade is necessary by verifying the current IOS version number. The IOS version number can be found in the output of the following commands:

show running-config

show version

show flash

The copy running-config flash memory command is incorrect because this command would copy the running configuration to the router's flash memory. It is the opposite of the copy flash-running config command. While this can be done, it is not a common practice. Flash is typically used to store the Cisco IOS or operating system. Configuration files are normally stored in NVRAM.

The copy startup-config tftp command is incorrect because this command would be used to copy the current configuration stored in NVRAM to a TFTP server. When you execute this command, you will be prompted for the IP address or hostname of the TFTP server. This prompt will display as below:

router#copy start tftp

Address or name of remote host []? 192.168.1.5

Destination filename [router-confg]?

The address 192.168.1.5 is the address of the TFTP server. If no file name is given, it will save the file as router-config.

The copy tftp running-config is incorrect. This command is used to merge a backup configuration located on a TFTP server with the configuration in RAM.

The copy running-config tftp command in incorrect. It is used to make a backup copy of the configuration residing in RAM to a TFTP server.

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Tech Notes > How To Copy a System Image from One Device to Another > Document ID: 15092

Cisco Documentation > Cisco IOS Release 12.4 Command References > Using Cisco IOS Software for Release 12.4 > Understanding Command Modes

Question 203

As part of a new initiative to tighten the security of your Cisco devices, you have configured the firewall to restrict access to the devices from the outside.

What would be other recommended ways of protecting the integrity of the device configuration files on the devices while ensuring your continued ability to manage the devices remotely? (Choose all that apply.)

- ☐ encrypt the configuration files
- ☒ use SSH to connect to the devices for management
- ☐ prevent the loss of administrator passwords by disabling their encryption
- ☐ disable the VTY ports on the devices
- ☒ use an encrypted password for VTY access

Explanation:

Explanation:

You should use SSH to connect to the devices for management. You should also require an encrypted password for VTY access. Using Telnet for remote management transmits all information, including the username and passwords, in clear text. Using an encrypted password for VTY access ensures that the password cannot be read either in transit or in the configuration file.

Passwords used for access to the console, aux, or VTY connections can be encrypted if desired. When passwords are created with the enable <password> command, the password is saved in clear text. When the enable secret <password> command is used, however the password will be encrypted.

If both types of password are configured for a particular connection type, the system will ignore the enable password and require the enable secret password. For example, if the set of commands shown below were executed, both types of password will be created for console access, but the system will require the password crisco rather than cisco. Also make note that neither of those passwords will required for VTY access. That password is sicso, which is the password configured after accessing the line VTY interface configuration prompt.

Router(config)# enable secret crisco

Router(config)# enable password cisco

Router(config)# line vty 0 4

 Licensed to Berend Post berend.post@it-university.nl

Router(config-line)# password sisco

Although it is possible to encrypt the password in the configuration files, it is not possible to encrypt the rest of the files.

You should not disable the encryption of the passwords in the configuration files. Password encryption is a good security measure to take, and sloppy password management should not be a reason to change this practice.

You should not disable the VTY ports on the devices. This would certainly enhance security, but it would prevent you from managing the devices remotely

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco IOS Security Configuration Guide, Release 12.2>Security Overview

Question 204

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

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

Explanation:

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.

 Licensed to Berend Post berend.post@it-university.nl

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

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

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco Documentation > Cisco IOS Security Command Reference, Release 12.4 > service password-encryption

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

Question 205

You set up several routers in your lab. Two of them are connected back to back using Data Terminal Equipment (DTE)-to-Data Circuit-terminating Equipment (DCE) cable. You need to configure the clock rate.

On which router would you configure the clock rate?

- ☒ the DCE
- ☐ the DTE
- ☐ The clock rate is set by default
- ☐ The clock rate cannot be configured

Explanation:

Explanation:

The clock rate is set on the Data Circuit-terminating Equipment (DCE) device. DCE is also known as Data Communications Equipment.

DCE terminates a physical WAN connection and provides clocking and synchronization of a connection between two locations and connects to a DTE. The DCE category includes equipment such as CSU/DSUs and modems. If you were connecting a router to a WAN link, the router would be the DTE end and would be connected to a CSU/DSU or a modem. Either of these devices would provide the clocking.

 Licensed to Berend Post berend.post@it-university.nl

DTE is an end-user device, such as a router or a PC that connects to the WAN via the DCE device.

Other options are incorrect. By default, no clock rate is configured, but can be set on a DCE device by using the clock rate [bps] command.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Question 206

You are the network administrator for your company. You have been assigned the task of configuring an appropriate IP addressing scheme in the network.

Assuming that the network address is 192.16.100.0/28, what will be the number of hosts per network in this scenario?

- ☐ 2
- ☐ 6
- ☒ 14
- ☐ 30

Explanation:

Explanation:

In this scenario, there will be 14 hosts per network. The formula for calculating the number of hosts on a subnet is 2n - 2, where n is the number of host bits in the summary mask. The n can be calculated by subtracting host bits from the total number of bits in a subnet mask (32). In this case, n would be 32 - 28 = 4. Therefore, the formula to calculate the number of bits in this scenario would be:

2(32 -28) - 2 = 24 - 2 = 14 hosts

You always subtract 2 from 2n because the all-zero-bit address is reserved for the network address (called the network ID) and the all-one-bit address is reserved for the broadcast address.

 Licensed to Berend Post berend.post@it-university.nl

The 192.16.100.0/28 network address would not have 30 hosts per network. The 192.16.100.0/27 network address would actually yield 30 hosts per network. In this case, n would be 32 - 27 = 5, so the number of host bits in the subnet mask would be 32 - 2, which is equal to 30.

The 192.16.100.0/28 network address would not have 6 hosts per network. The 192.16.100.0/29 network address would yield 6 hosts per network. In this case, n would be 32 - 29 = 3, so the number of host bits in the subnet mask would be 8 - 2, which is equal to 6.

The 192.16.100.0/28 network address would not have 2 hosts per network. The 192.16.100.0/30 network address would yield 2 hosts per network. In this case, n would be 32 - 30 = 2, so the number of host bits in the subnet mask would be 4 - 2, which is equal to 2.

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Cisco > Technology Support > IP > IP Routing > Design Technotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Question 207

Which command is used to disable Cisco Discovery Protocol (CDP) on a Cisco router?

- ☐ disable cdp
- ☒ no cdp run
- ☐ no cdp enable
- ☐ no cdp advertise-v2

Explanation:

Explanation:

The no cdp run command is used to disable CDP on a Cisco router globally. CDP is a Layer 2 (Data Link layer) protocol that discovers information about neighboring network devices. CDP does not use network layer protocols to transmit information because it operates at the Data Link layer. Therefore, it is useful to determine information about directly connected Cisco network devices, because it can operate when network protocols have not been configured or are misconfigured. The show cdp neighbors detail command is used to view the IP addresses of the directly connected Cisco devices.

 Licensed to Berend Post berend.post@it-university.nl

The no cdp advertise-v2 command disables CDPv2 advertisements. It will not disable the protocol globally.

The no cdp enable command is used to disable CDP on an interface. In a situation where CDP needs to be disabled on a single interface only, such as the interface leading to the Internet, this command would be executed from interface configuration mode for that specific interface. It will not disable the protocol globally. For example, to disable CDP for only the serial0 interface, the command sequence would be:

Router#configure terminal

Router(config)#interface serial 0

Router(config-if)no cdp enable

The disable cdp command is not a valid Cisco command.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Cisco IOS Network Management Command Reference > show cdp neighbors

Question 208

What command produced the following as a part of its output?

1 14.0.0.2 4 msec 4 msec 4 msec
2 63.0.0.3 20 msec 16 msec 16 msec
3 33.0.0.4 16 msec * 16 msec

- ☐ Ping
- ☒ Traceroute
- ☐ Tracert
- ☐ Extended ping

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The output displayed is a part of the output from executing the traceroute command. The traceroute command finds the path a packet takes while being transmitted to a remote destination. It is also used to track down routing loops or errors in a network. Each of the following numbered sections represents a router being traversed and the time the packet took to go through the router:

1 14.0.0.2 4 msec 4 msec 4 msec

2 63.0.0.3 20 msec 16 msec 16 msec

3 33.0.0.4 16 msec * 16 msec

The output would not be displayed by the ping command. This command is used to test connectivity to a remote ip address. The output from the ping command is as follows:

router1# ping 10.201.1.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.201.1.11, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

The ping in this output was unsuccessful, as indicated by the Success rate is 0 percent output.

The output would not be displayed by the tracert command. The tracert command is used by Microsoft Windows operating systems, not the Cisco IOS command line interface. However, the purpose of the tracert command is similar to the Cisco traceroute utility, which is to test the connectivity or "reachability" of a network device or host. The tracert command uses Internet Control Message Protocol (ICMP).

The output would not be displayed by the extended version of the ping command. This command can be issued on the router to test connectivity between two remote routers. A remote execution means that you are not executing the command from either of the two routers you are interested in testing, but from a third router.

To execute an extended ping, enter the ping command from the privileged EXEC command line without specifying the target IP address. The command takes the router into configuration mode, where you can define various parameters, including the destination and target IP addresses. An example is below:

 Licensed to Berend Post berend.post@it-university.nl

Protocol [ip]:

Target IP address: 10.10.10.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 12.1.10.2

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Each line is a menu question allowing you to either accept the default setting (in parenthesis) of the ping or apply a different setting. The real value of this command is that you can test connectivity between two remote routers without being physically present at those routers, as would be required with the standard version of the ping command.

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > ping

Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730 > The Extended ping Command

Licensed to Berend Post berend.post@it-university.nl

Question 209

What will be the effect of executing the following command on port F0/1?

switch(config-if)# switchport port-security mac-address 00C0.35F0.8301

- ☒ The command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port.
- ☐ The command expressly prohibits the MAC address of 00c0.35F0.8301 as an allowed host on the switch port.
- ☐ The command configures an inbound access control list on port F0/1 limiting traffic to the IP address of the host.
- ☐ The command encrypts all traffic on the port from the MAC address of 00c0.35F0.8301.

Explanation:

Explanation:

The command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port. By default, an unlimited number of MAC addresses can be learned on a single switch port, whether it is configured as an access port or a trunk port. Switch ports can be secured by defining one or more specific MAC addresses that should be allowed to connect, and violation policies (such as disabling the port) if additional hosts try to gain a connection.

The switchport port-security mac-address 00C0.35F0.8301 command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port.

The switchport port-security mac-address 00C0.35F0.8301 command does not expressly prohibit the MAC address of 00c0.35F0.8301 as an allowed host on the switch port. The port-security command is designed to identify allowed MAC addresses not prohibited addresses.

The switchport port-security mac-address 00C0.35F0.8301 command does not configure an inbound access control list on port F0/1 limiting traffic to the IP address of the host. It will accept traffic to the port, but will only allow a device with that MAC address to be connected to the port.

The switchport port-security mac-address 00C0.35F0.8301 command does not encrypt all traffic on the port from the MAC address of 00c0.35F0.8301. The port-security command has nothing to do with encryption.

Objective:

Infrastructure Security

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Configure, verify, and troubleshoot port security

References:

Cisco > Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide > Configuring Port Security > Enabling Port Security

Cisco > Support > Cisco IOS Security Command Reference: Commands S to Z > switchport port-security mac-address

Question 210

You apply the following commands to a router named R2:

```
R2(config)# interface Tunnel1
R2(config-if)# ip address 172.16.1.2 255.255.255.0
R2(config-if)# ip mtu 1400
R2(config-if)# ip tcp adjust-mss 1360
R2(config-if)# tunnel source 2.2.2.2
R2(config-if)# tunnel destination 1.1.1.1
```

Which statement is NOT true with regard to this configuration?

- ☐ The physical IP address of R2 is 2.2.2.2
- ☐ The connection will operate in IP mode
- ☒ The configuration will increase packet fragmentation
- ☐ The configuration alters the maximum segment size

Explanation:

Explanation:

The configuration will not increase packet fragmentation. Conversely, it will reduce it by lowering the maximum transmission unit to 1400 and the maximum segment size to 1360 bytes.

Most transport MTUs are 1500 bytes. Simply reducing the MTU will account for the extra overhead added by GRE. Setting the MTU to a value of 1400 is a common practice, and it will ensure unnecessary packet fragmentation is kept to a minimum.

The other statements are true. The physical address of R2 is 2.2.2.2, while the tunnel interface address is 172.16.1.2.

Because you have not issued any command that changes the connection, it will operate in the default mode of IP.

Licensed to Berend Post berend.post@it-university.nl

The configuration does alter the maximum segment size with the ip tcp adjust-mss 1360 command.

Objective:

WAN Technologies

Sub-Objective:

Configure, verify, and troubleshoot GRE tunnel connectivity

References:

Home > Network Infrastructure > WAN, Routing and Switching > How to configure a GRE tunnel

Question 211

You are configuring all your devices for IPv6. Which of the following is the only device that requires the ipv6 unicast-routing command?

- ☐ Layer 2 switch
- ☒ Router
- ☐ Adaptive security appliance
- ☐ Wireless AP

Explanation:

Explanation:

Only the router requires the ipv6 unicast-routing command. The command ipv6 unicast-routing enables the routing of IPv6 packets on a router. It is not required when you are simply configuring interfaces on devices that participate in IPv6.

A Layer 2 switch can have an IPv6 address applied to its management interface and to any VLAN interfaces. However, because the switch does no routing, it does not require the ipv6 unicast-routing command.

An adaptive security appliance (ASA) can also have IPv6 addresses applied to its interfaces and can route both IPv6 and IPv4 traffic. However, it does not require the ipv6 unicast-routing command.

A wireless access point differs from a wireless router in that it operates as a switch or hub and does no routing. Therefore, it does not require this command.

Objective:

Network Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure, verify, and troubleshoot IPv6 addressing

References:

Cisco > Support > IPv6 Configuration Guide, Cisco IOS Release 15.2S > Chapter: IPv6 Unicast Routing

Cisco > Support > Cisco IOS IPv6 Command Reference > ipv6 unicast-routing

Question 212

Which of the following are NOT valid IPv6 addresses? (Choose all that apply.)

- ☒ 225.1.4.2
- ☐ ::FFFF:10.2.4.1
- ☐ ::
- ☐ 2001:0:42:3:ff::1
- ☒ fe80:2030:31:24
- ☐ 2001:42:4:0:0:1:34:0
- ☐ 2003:dead:bef:4dad:ab33:46:abab:62

Explanation:

Explanation:

The addresses 255.1.4.2 and fe80:2030:31:24 are not valid IPv6 addresses.

225.1.4.2 is incorrect because it is an IPv4 multicast address. The address fe80:2030:31:24 is incorrect because it does not represent a 16-byte IPv6 address, with colons separating each 2-byte segment.

IPv6 addresses are 16 bytes, or 128 bits in length. The following are valid IPv6 addresses.

::FFFF:10.2.4.1 is an example of an IPv4-compatible IPv6 address, where the first 10 bytes (80 bits) of the address are set to 0 the next 2 bytes (16 bits) are set to FFFF and the last 32 bits are the IPv4 address

:: is the IPv6 "unspecified address." It is a unicast address not assigned to any interface, and is used by a DHCP-dependent host prior to allocating a real IPv6 address.

2001:0:42:3:ff::1 is a valid IP address, with the :: representing two segments (4 bytes) of compressed zeros.

2001:42:4:0:0:1:34:0 is a valid IP address, with only the leading zeros of each segment truncated.

 Licensed to Berend Post berend.post@it-university.nl

2003:dead:beef:4dad:ab33:46:abab:62 has 16 bytes, is divided correctly by colons into eight sections, utilizes the dropping of leading zeros in each section correctly, and uses the letters a-f in the three section that spell out dead beef 4 dad.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast IPv6 address types

References:

Cisco > Technology Support > IP > IPv6 > Technology Information > Technology White Paper > IPv6 Addressing At A Glance (PDF)

Cisco > Internetworking Technology Handbook > IPv6

Question 213

What is the broadcast address for subnet 172.25.4.0/23?

- ☐ 172.25.4.255
- ☒ 172.25.5.255
- ☐ 172.25.6.255
- ☐ 172.25.7.255

Explanation:

Explanation:

The broadcast address for subnet 172.25.4.0/23 will be 172.25.5.255.

When using a mask of /23, the subnet mask is 255.255.254.0. This means that the interval, or block size, of each subnet is 2, and that it will be incremented in the third octet. Therefore, the next network ID after 172.25.4.0 will be 172.25.6.0. Since the broadcast address of each subnet is the last address in that subnet before the next network ID, the broadcast address will be 172.25.5.255.

172.25.4.255 is a valid address in the 172.25.4.0/23 network, since the network range is 172.25.4.1 - 172.25.5.254.

172.25.6.255 is a valid address in the 172.25.6.0/23 network. Its range is 172.25.6.1 -172.25.7.254. Since the next network ID after 172.25.6.0 is 172.25.8.0, as the interval is 2 and it is incremented in the third octet, the broadcast address would be 172.25.7.255.

Licensed to Berend Post berend.post@it-university.nl

For the same reason, 172.25.6.255 is the broadcast address for the 172.25.6.0/24 network.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco > Design Tech Notes > IP Routing > IP Addressing and Subnetting for New Users > Understanding IP Addresses > Document ID: 13788

Question 214

On which of the following networks will OSPF elect a designated router (DR)? (Choose two.)

- ☒ Broadcast
- ☒ NBMA
- ☐ Point-to-point
- ☐ Point-to-multipoint

Explanation:

Explanation:

OSPF will perform an election for a designated router (DR) and backup designated router (BDR) on every multi-access network segment. Multi-access segments are defined as segments where more than two hosts can reach each other directly, such as a shared Ethernet segment (broadcast multi-access) or Frame Relay (non-broadcast multi-access, or NBMA).

DR and BDR elections do not occur on point-to-point or point-to-multipoint segments. Point-to-point and point-to-multipoint segments are not considered multi-access segments. OSPF routers on these network types will establish an adjacency without a DR/BDR election.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

 Licensed to Berend Post berend.post@it-university.nl

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039 > DR Election

Question 215

Which Cisco IOS command can be issued on a router to test the connectivity of one interface from another interface on the same router?

- ☒ ping (with no address specified)
- ☐ ping (with an address specified)
- ☐ tracert
- ☐ traceroute

Explanation:

Explanation:

The extended ping Cisco IOS utility, which is issued with no address specified, can be issued on a router to test connectivity between two remote routers. The ping utility uses Internet Control Messaging Protocol (ICMP) packets. An ICMP echo request is sent to the destination host. Upon its receipt, the destination host responds to the sending host with an ICMP echo reply. When the echo reply is received, the connectivity is verified. Below is sample output of the extended ping command:

```
Router R#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 12.1.10.2
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

The ping command with an address specified is incorrect because you when you issue this command you will either receive a reply from the destination or a destination unreachable message. It will not prompt for additional information as shown which is what allows you to specify the endpoints for the ping.

The traceroute command is not correct for this scenario because this command traces the path between the host issuing the command and the target network.

The tracert command is not a Cisco IOS command, but a Microsoft command.

 Licensed to Berend Post berend.post@it-university.nl

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

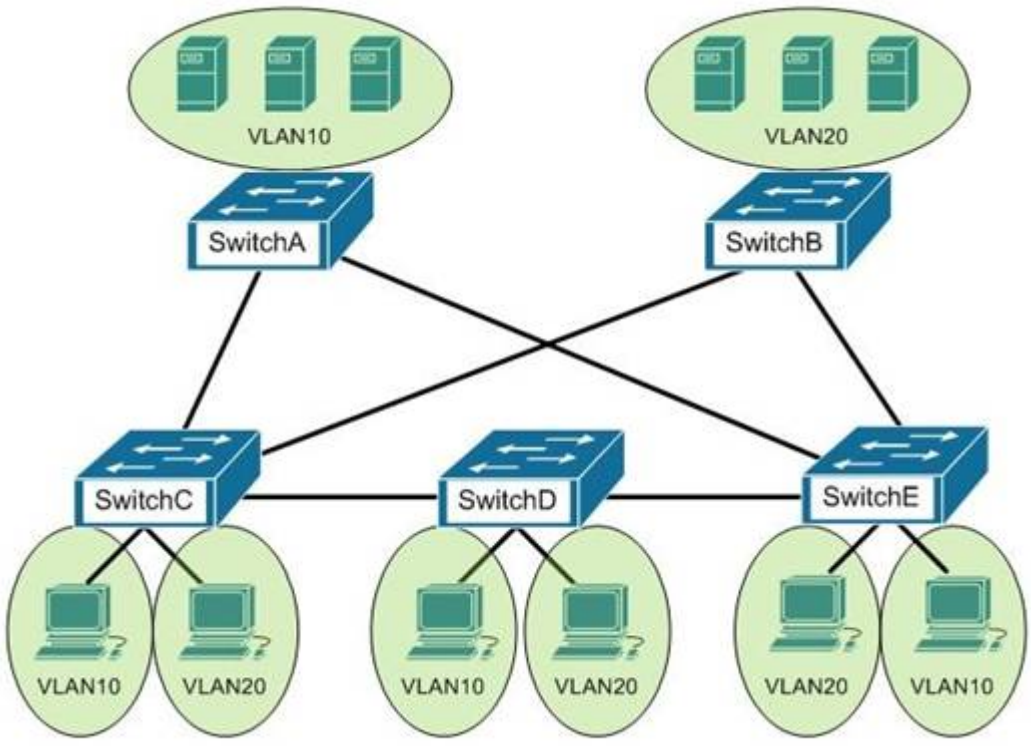
Cisco > Tech Notes > Using the Extended ping and Extended traceroute Commands > Document ID: 13730 > The Extended ping Command

Cisco > Cisco IOS Command Fundamentals Reference, Release 12.4 > ping

Licensed to Berend Post berend.post@it-university.nl

Question 216

You are the switch administrator for InterConn. The network is physically wired as shown in the diagram. You are planning the configuration of STP. The majority of network traffic runs between the hosts and servers within each VLAN.



You would like to designate the root bridges for VLANS 10 and 20. Which switches should you designate as the root bridges?

- ☐ Switch A for VLAN 10 and Switch E for VLAN 20
- ☒ Switch A for VLAN 10 and Switch B for VLAN 20
- ☐ Switch A for VLAN 10 and Switch C for VLAN 20
- ☐ Switch D for VLAN 10 and Switch B for VLAN 20
- ☐ Switch E for VLAN 10 and Switch A for VLAN 20
- ☐ Switch B for VLAN 10 and Switch E for VLAN 20

Explanation:

Explanation:

You should designate Switch A for VLAN 10 and Switch B for VLAN 20. The STP root bridge for a particular VLAN should be placed as close as possible to the center of the VLAN. If the majority of network traffic is between the hosts and servers within each VLAN, and the servers are grouped into a server farm, then the switch that all hosts will be sending their data to is the ideal choice for the STP root. Cisco's default implementation of STP is called Per-VLAN Spanning Tree (or PVST), which allows individual tuning of the spanning tree within each VLAN. Switch A can be configured as the root bridge for VLAN 10, and Switch B can be configured as the root bridge for VLAN 20, resulting in optimized traffic flow for both.

Licensed to Berend Post berend.post@it-university.nl

None of the other switches is in the traffic flow of all data headed towards the VLAN 20 or VLAN 10 server farms, so they would not be good choices for the root bridge for either VLAN. Care should be taken when adding any switch to the network. The addition of an older, slower switch could cause inefficient data paths if the old switch should become the root bridge.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and TechNotes > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

Question 217

Which Cisco Internetwork Operating System (IOS) command is used to save the running configuration to non-volatile random access memory (NVRAM)?

- ☐ copy startup-config running-config
- ☐ move startup-config running-config
- ☒ copy running-config startup-config
- ☐ move startup-config running-config

Explanation:

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.

 Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

Cisco Documentation > RPM Installation and Configuration > IOS and Configuration Basics

Question 218

Which command is NOT mandatory for inclusion in a plan to implement IP Service Level Agreements (SLAs) to monitor IP connections and traffic?

- ☐ ip sla
- ☐ ip sla schedule
- ☒ ip sla reset
- ☐ icmp-echo

Explanation:

Explanation:

The ip sla reset command is not mandatory for an implementation plan to configure IP SLAs for monitoring IP connections and traffic. This command causes the IP SLA engine to either restart or shutdown. As a result, all IP SLAs operations are stopped, IP SLA configuration information is erased, and IP SLAs are restarted. The IP SLAs configuration information will need to be reloaded to the engine.

The following commands are essential to the implementation plan:

ip sla

ip sla schedule

icmp-echo

The ip sla command allows you to configure IP SLAs operations. When you execute this command in the global configuration mode, it enables the IP SLA configuration mode. In the IP SLA configuration mode, you can configure different IP SLA operations. You can configure up to 2000 operations for a given IP SLA ID number.

 Licensed to Berend Post berend.post@it-university.nl

The icmp-echo command allows you to monitor IP connections and traffic on routers by creating an IP SLA ICMP Echo operation. This operation monitors end-to-end response times between routers.

The ip sla schedule command allows you to schedule the IP SLA operation that has been configured. With this command, you can specify when the operation starts, how long the operation runs, and the how long the operation gathers information. For example, if you execute the ip sla schedule 40 start-time now life forever command, the IP SLA operation with the identification number 40 immediately starts running. This is because the now keyword is specified for the start-time parameter. Using the forever keyword with the life parameter indicates that the operation keeps collecting information indefinitely. Note that you cannot re-configure the IP SLA operation after you have executed the ip sla schedule command.

The information gathered by an IP SLA operation is typically stored in RTTMON-MIB. A Management Information Base (MIB) is a database hosting information required for the management of routers or network devices. The RTTMON-MIB is a Cisco-defined MIB intended for Cisco IOS IP SLAs. RTTMON MIB acts as an interface between the Network Management System (NMS) applications and the Cisco IOS IP SLAs operations.

Objective:

Infrastructure Management

Sub-Objective:

Troubleshoot network connectivity issues using ICMP echo-based IP SLA

References:

Home > Support > Technology support > IP > IP application services > Technology information > Technology white paper > Cisco IOS IP Service Level Agreements User Guide

Cisco IOS IP SLAs Command Reference > icmp-echo through probe-packet priority > ip sla

Cisco IOS IP SLAs Command Reference > icmp-echo through probe-packet priority > ip sla schedule

Cisco > Cisco IOS IP SLAs Command Reference > icmp-echo

Licensed to Berend Post berend.post@it-university.nl

Question 219

What is the default Administrative Distance (AD) value for an Enhanced Interior Gateway Routing Protocol (EIGRP) summary route?

- ☐ 1
- ☒ 5
- ☐ 90
- ☐ 20

Explanation:

Explanation:

The default Administrative Distance (AD) value for an Enhanced Interior Gateway Routing Protocol (EIGRP) summary route is 5. The following table shows the AD values for different protocols and their IP routes:

IP Route	Default AD value
Connected interface	0
Static route directed to an connected interface	0
Static route directed to an IP address	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP) route	20
Internal Enhanced Interior Gateway Routing Protocol (EIGRP) route	90
Interior Gateway Routing Protocol (IGRP) route	100
Open Shortest Path First (OSPF) route	110
Intermediate System-to-Intermediate System (IS-IS) route	115
Routing Information Protocol (RIP) route	120
Exterior Gateway Protocol (EGP) route	140
On Demand Routing (ODR)	160
External Enhanced Interior Gateway Routing Protocol (EIGRP) route	170
Internal Border Gateway Protocol (BGP) route	200
Unknown origin routes	255

The option 1 is incorrect because this is the default AD value for static routes.

The option 90 is incorrect because this is the default AD value for internal EIGRP routes.

The option 20 is incorrect because this is the default AD value for external BGP routes.

Objective:

Routing Fundamentals

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Compare and contrast interior and exterior routing protocols

References:

Question 220

Which of the following is NOT a mode of Dynamic Trunking Protocol (DTP)?

- ☐ dynamic auto
- ☒ dynamic trunk
- ☐ dynamic desirable
- ☐ nonegotiate

Explanation:

Explanation:

Dynamic trunk is not a DTP mode. DTP is a Cisco proprietary trunk negotiation protocol and is used to determine if two interfaces on connected devices can become a trunk. There are five modes of DTP:

Trunk: Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not agree to the change.

Access: Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface does not agree to the change.

Dynamic desirable: Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.

Dynamic auto: Makes the interface willing to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. This is the default mode for all Ethernet interfaces in Cisco IOS.

Nonegotiate: Puts the interface into permanent trunking mode but prevents the interface from generating DTP frames. You must configure the neighboring interface manually as a trunk interface to establish a trunk link. Use this mode when connecting to a device that does not support DTP.

If one side's mode of link is in trunk mode, dynamic desirable mode, or dynamic auto mode, and the other side is trunk or dynamic desirable, a trunk will form. Nonegotiate mode enables trunking but disables DTP.

Objective:

LAN Switching Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Question 221

Which Enhanced Interior Gateway Routing Protocol (EIGRP) packet is NOT sent reliably over the network?

- ☐ Update
- ☐ Query
- ☐ Reply
- ☒ Acknowledgement

Explanation:

Explanation:

Acknowledgement packets are sent unreliably over the network, and there is no guaranteed delivery of acknowledgement packets between neighboring routers.

Acknowledgement packets are a special type of hello packets that do not contain data and have a non-zero acknowledgement number. These are sent as a unicast.

Update, Query, and Reply packets use Reliable Transport Protocol (RTP), which ensures guaranteed delivery of packets between neighboring devices. The RTP mechanism ensures loop-free synchronized network.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Internetworking Technology Handbook > Enhanced Interior Gateway Routing Protocol (EIGRP)

Licensed to Berend Post berend.post@it-university.nl

Question 222

File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP) work at which layer in the Open Systems Interconnection (OSI) model?

- ☐ the Session layer
- ☐ the Presentation layer
- ☒ the Application layer
- ☐ the Network layer

Explanation:

Explanation:

FTP and SMTP work at the application layer in the OSI model. The application layer is responsible for interacting directly with the application. It provides application services, such as e-mail and FTP. The following protocols work on the application layer:

FTP: Used to transfer data between hosts through the Internet or a network.

SMTP: A Transmission Control Protocol (TCP)/ Internet Protocol (IP) protocol used to send and receive e-mail messages.

Telnet: Used to allow remote logins and command execution.

The Session layer is incorrect because this layer creates, manages, and terminates sessions between communicating nodes. NetBIOS and Session Control Protocol (SCP) work at the session layer.

The Presentation layer is incorrect because this layer enables coding and conversion functions for application layer data. The Presentation layer includes graphic image formats, such as Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF).

The Network layer is incorrect because this layer defines the network address or the Internet Protocol (IP) address, which are then used by the routers to make forwarding decisions.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast OSI and TCP/IP models

References:

Cisco Documentation > Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems

Licensed to Berend Post berend.post@it-university.nl

Question 223

A new switch is added to the network, and several production VLANs are shut down.

Which of the following is a probable cause for this scenario? (Choose two.)

- ☐ The new switch has a lower configuration revision number than existing switches.
- ☒ The new switch has a higher configuration revision number than existing switches.
- ☐ The new switch is operating in transparent mode.
- ☒ The new switch is operating in server mode.

Explanation:

Explanation:

The VLAN database of the new switch will overwrite the VLAN databases of the production switches because it is operating in server mode and has a higher VLAN configuration revision number. The VLAN Trunking Protocol (VTP) is used to synchronize VLANs between different switches. The VTP configuration revision number is used to determine which VTP switch has the most current version of the VLAN database, and is incremented whenever a VLAN change is made on a VTP server switch. The show vtp status command is used to view the configuration revision number, as shown in this sample output:

Switch# show vtp status

VTP Version : 2

Configuration Revision : 62

Maximum VLANs supported locally : 1005

Number of existing VLANs : 24

VTP Operating Mode : Server

VTP Domain Name : Corporate

VTP Pruning Mode : Enabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80

This switch has a configuration revision number of 62, which will be compared to other switches in the same VTP domain. If the production switches have a lower configuration revision number than the new switch, their VLAN databases will be replaced with the VLAN database of the new switch. This could mean that VLANs that formerly existed on those production switches may be deleted. Any switch ports that had been assigned to VLANs that become deleted will be disabled, possibly resulting in catastrophic network failure. All VTP switches in the same VTP domain should have a

 Licensed to Berend Post berend.post@it-university.nl

domain password defined, which will protect against a rogue switch being added to the network and causing VLAN database corruption.

The new switch does not have a lower configuration revision number, since this would cause the new switch to have its VLAN database replaced with the existing production VLANs. This would not cause the problem described in the scenario.

The new switch is not operating in transparent VTP mode because a switch operating in transparent VTP mode will never synchronize its VLAN database with other switches.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Cisco > Support > LAN Switching > Virtual LANS / VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Configuring VLAN Trunk Protocol (VTP) > Document ID: 98154

Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25) > Understanding and Configuring VLANs, VTP, and VMPS

Question 224

Which Cisco command will display the version and configuration data for Secure Shell (SSH)?

- ☐ show ssh
- ☒ show ip ssh
- ☐ debug ssh
- ☐ debug ip ssh

Explanation:

Explanation:

The show ip ssh command is used to display the version and configuration data for SSH on a Cisco router. The following is sample output of the show ip ssh command:

router#show ip ssh

SSH Enabled - version 1.5

Licensed to Berend Post berend.post@it-university.nl

Authentication timeout: 120 secs; Authentication retries: 2

This show ip ssh command output displays the enabled status of the SSH protocol, the retries parameter (configured at two attempts), and the timeout of 120 seconds.

The following message will appear when the show ip ssh command is issued and SSH has been disabled:

router# show ip ssh

%SSH has not been enabled

To enable SSH include the transport input SSH command when configuring authentication on a line. For example, the configuration of a Cisco network device to use SSH on incoming communications via the virtual terminal ports, with a specified password as shown from the partial output of the show run command is shown below:

line vty 0 4

password 7 030752180500

login

transport input ssh

It is important to note the login command on the third line of the above ouput is critical for security. This command instructs the device to prompt for a username and password using SSH. If this line reads no login, SSH might be otherwise be correctly configured, but the device will never prompt for the username and password.

The show ssh command will display the status of the SSH connections on the router The following is the sample output of the show ssh command:

```
router# show ssh
Connection Version Encryption      State               Username
     0     1.5      3DES           Session Started           tim
```

The debug ip ssh command is used to display debug messages for SSH.

The debug ssh command is not a valid Cisco command.

 Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Cisco > Cisco IOS Security Command Reference > show ip ssh

Question 225

Which two statements are TRUE of Internet Protocol (IP) addressing? (Choose two.)

- ☒ Public addresses are registered with the Internet Assigned Numbers Authority (IANA).
- ☐ These addresses are publicly registered with the Internet Service Provider (ISP).
- ☒ Through a public IP address, you can access another computer on the Internet, such as a Web server.
- ☐ The ranges of public IP addressing are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.
- ☐ Private addresses are allocated by the Internet Assigned Numbers Authority (IANA).

Explanation:

Explanation:

Public addresses are publicly registered with the Internet Assigned Numbers Authority (IANA). Through a public IP address, you can access an Internet computer like a Web server.

The following statements are true of public IP addressing:

These addresses are publicly registered with the Internet Assigned Numbers Authority (IANA)

Through a public IP address, you can access another Internet computer, such as a Web server.

Other people on the Internet can obtain information about or access to your computer via a public IP address.

Public IP addresses are visible to the public.

The option stating that public IP addresses are publicly registered with the Internet Service Provider (ISP) is incorrect. Public IP addresses are registered with the Internet Assigned Numbers Authority (IANA). Since 1998, InterNIC has been primarily responsible for allocating domain names and IP addresses under the governance of the Internet Corporation for Assigned Names and Numbers (ICANN) body, a U.S. non-profit corporation that was created to oversee work performed by the Internet Assigned Numbers Authority (IANA).

Licensed to Berend Post berend.post@it-university.nl

The option stating that 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255 are the range of public IP addressing is incorrect. These ranges belong to private IP addressing.

The option stating that private addresses are allocated by the IANA is incorrect. Private IP address are not managed, but are used by private organizations as they see fit. The IANA is governed by ICANN, and its primarily role is to allocate overseas global IP addresses from the pools of unallocated addresses, as well as DNS root zone management.

Objective:

Network Fundamentals

Sub-Objective:

Describe the need for private IPv4 addressing

References:

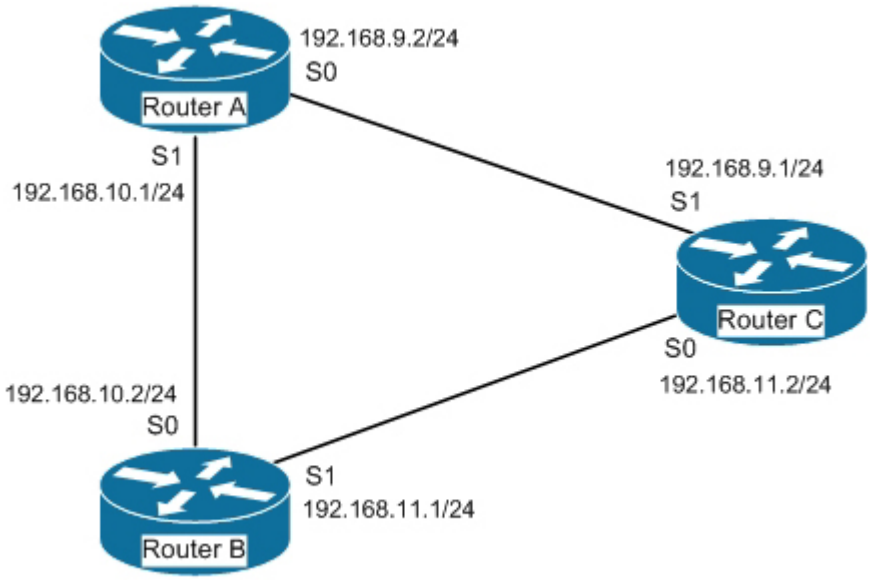
Cisco > Support > IP Addressing

http://www.debianadmin.com/private-and-public-ip-addresses-explained.html

Licensed to Berend Post berend.post@it-university.nl

Question 226

You have three EIGRP routers that are connected as shown in the diagram below.



Router A and Router C do not seem to be exchanging information. You execute commands on all three routers, and receive as output the information shown below:

```
Router A# show ip eigrp neighbors
Address Interface holdtime uptime Q Seq SRTT RTO
192.168.10.2 S1 13 1:20:10 100 458 0 30

routerA# show run              routerC# show run
<output omitted>               <output omitted>
router eigrp 56                router eigrp 56
network 192.168.10.0           network 192.168.11.0
network 192.168.9.0            no auto-summary
no auto-summary
```

What needs to be done to make Routers A and C start exchanging information?

- ☐ Execute the auto-summary command on Router A
- ☒ Execute the network 192.168.9.0 command under EIGRP 56 on Router C
- ☐ Correct the IP address on the S1 interface of Router C
- ☐ Recreate the EIGRP configuration on Router C as EIGRP 55

Explanation:

Explanation:

Router C is not displayed in the neighbor table of Router A, which indicates that Router C and Router A are not forming a neighbor relationship or exchanging information. This is because Router C does not have EIGRP configured for its S1 interface. You can see this is missing from its configuration in the output of the show run command for RouterC. To solve the issue, you should execute the network

Licensed to Berend Post berend.post@it-university.nl

192.168.9.0 command under the EIGRP 56 configuration on Router C. Then Router C will start sending hellos on that interface and the two routers will become neighbors.

The show ip eigrp neighbors command displays the following information for each EIGRP neighbor. In parentheses is the value of each found in the output of router A for Router B:

IP address (192.168.10.2)

Local interface (S1)

Retransmit interval (13)

Queue count (100)

There is no need to execute the auto-summary command on Router A. It will not affect the establishment of a neighbor relationship between Routers A and C.

There is no need to correct the IP address on the S1 interface of Router C. The address 192.168.9.1 is correctly located in the same subnet as the address on S0 of Router A.

Finally, changing the EIGRP configuration on Router C to EIGRP 55 will not help. Router C will not start sending hellos on its S1 interface until EIGRP is enabled on the S1 interface. Until then, the Routers A and C will not form a neighbor relationship and will not share information.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Cisco IOS IP Routing Configuration Guide, Release 12.4 > Configuring EIGRP > Enabling EIGRP

Licensed to Berend Post berend.post@it-university.nl

Question 227

You are the network administrator for your company. You have a Class B address range and are planning for a network that allows 150 hosts per subnet and at least 164 subnets.

Which subnet mask should you use to accomplish the task?

- ☐ 255.255.192.0
- ☐ 255.255.255.192
- ☒ 255.255.255.0
- ☐ 255.255.255.252

Explanation:

Explanation:

You should use 255.255.255.0 as the subnet mask to allow 150 hosts per subnet and at least 164 subnets. The formulas used to calculate the number of subnets and hosts are:

Number of subnets = 2number-of-subnet-bits

Number of hosts per subnet = 2number-of-host-bits - 2

Subnet mask in decimal: 255.255.255.0

Subnet mask in binary: 11111111.11111111.11111111.00000000

Number of subnet bits: 8 (binary 1s in the subnet octet of the subnet mask)

Number of host bits: 8 (binary 0s in the subnet mask)

In this scenario, we find that for 255.255.255.0:

Subnets that can be used: 28 = 256

Hosts that can be used: 28 - 2 = 254

The other options do not allow 150 hosts per subnet and at least 164 subnets.

If you use 255.255.192.0 as the subnet mask, then the total number of hosts that can be connected per subnet is 16382 (214 - 2 = 16382). However, there will be 4 subnets (22 = 4).

If you use 255.255.255.192 as the subnet mask, there will be 62 hosts (26 - 2 = 62).

Licensed to Berend Post berend.post@it-university.nl

If you use 255.255.255.252 as the subnet mask, there will be two hosts per subnet (22 - 2 = 2).

Note: This mask is frequently used for a subnet that connects two routers. In that case, there are two interfaces in the subnet, and thus it is most efficient use of the addressing space. This is also the most efficient way to address a point-to-point serial link.

A note about the formulas: You will always subtract 2 from the number of hosts (2number-of-host-bits - 2) because the all-zeroes bit address is reserved for the network address and the all-ones bit address is reserved for the broadcast address.

Before Cisco IOS Software Release 12.0, it was common practice to subtract 2 from the networks formula (2number-of-subnet-bits) to exclude the all-ones subnet and subnet zero. Today that range is usable, except with some legacy systems. On certain networks with legacy software, you may need to use the previous formula (2number-of-subnet-bits - 2) to calculate the number of valid subnets.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Cisco > Technology Support > IP > IP Addressing Services > Design TechNotes > Subnet Zero and the All-Ones Subnet > Document ID: 13711

Question 228

Which of the following is a frame tagging method for identifying Virtual LAN (VLAN) memberships over trunk links?

- ☐ STP
- ☐ RIP
- ☐ CDP
- ☒ 802.1q

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

802.1q is a frame tagging method for identifying Virtual LAN (VLAN) memberships over trunk links. Frame tagging ensures identification of individual VLAN frames over a trunk link that carries frames for multiple VLANs. This frame tagging method is a standardized protocol developed by The Institute of Electrical and Electronics Engineers (IEEE). Cisco has also developed a proprietary frame tagging method, known as Inter-Switch Link (ISL).

When configuring a trunk link between a router and a switch, you must configure the physical interface on the router with one subinterface for each VLAN, and you must configure the physical ports on the router and the switch with the same encapsulation type, whether 802.1q or ISL.

Spanning Tree Protocol (STP) is not a frame tagging method, but a protocol used to remove switching loops in redundantly configured switched environments and create a single active Layer 2 path between any two network segments. Whenever a network segment can be handled by more than one switch, STP will elect one switch to take responsibility, and the other switches will be placed into a blocking state for the ports connected to that segment. In this way, only one switch receives and forwards data for this segment, removing the potential for generating multiple copies of the same frame. The benefits of STP include:

Prevention of broadcast storms

Prevention of multiple frame copies

Media Access Control (MAC) address database stability

Routing Information Protocol (RIP) is not a frame tagging method, but a distance vector routing protocol. It populates routing tables dynamically about the topology changes.

Cisco Discovery Protocol is not a frame tagging method, but a Cisco proprietary protocol used to collect hardware and protocol information for directly connected Cisco devices. CDP has nothing to do with VLANs.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Support > Technology Support > LAN Switching > Layer-Three-Switching and Forwarding > Configure > Configuration Examples and Technotes > Configuring InterVLAN Routing and ISL/802.1Q Trunking on a Catalyst 2900XL/3500XL/2950 Switch Using an External Router

Question 229

Which device will always have all of its ports in the same collision domain?

- ☒ Hub
- ☐ Bridge
- ☐ Switch
- ☐ Router

Explanation:

Explanation:

Open Systems Interconnect (OSI) Layer 1 devices, such as hubs and repeaters, do not create multiple collision domains. All of their ports remain in the same collision domain as well as the same broadcast domain.

A collision domain is a domain where two or more devices in the domain could cause a collision by sending frames at the same time. Each switch port is a separate collision domain. Replacing a hub with a switch effectively eliminates collisions for devices connected to the switch ports.

Bridges and switches create multiple collision domains and can reduce collisions within a broadcast domain, as each port constitutes a separate collision domain. However, if the network is not segmented with Virtual LANs (VLANs), all ports remain in the same broadcast domain. The main difference between a bridge and a switch is that the latter has a higher port capacity and better performance. VLANs segment the network into smaller broadcast domains using a Layer 2 device such as switch.

Routers segment the network into multiple broadcast domains. Routers are Layer 3 devices, and thus they interconnect different Layer 3 IP networks. Every interface/subinterface on a router has a unique IP network/subnet address that corresponds to a broadcast domain. Thus, every interface on a router defines a broadcast domain.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Internetworking Technology Handbook > Routing Basics

Question 230

Which Cisco Internetwork Operating System (IOS) command is used to view information about the Dynamic Host Configuration Protocol (DHCP) address pool?

- ☐ show ip dhcp server statistics
- ☒ show ip dhcp pool
- ☐ show dhcp pool
- ☐ show ip dhcp server pool

Explanation:

Explanation:

The show ip dhcp pool command is used to view information about the DHCP address pool. The following code is a sample output of this command:

```
Pool 1:
Utilization mark (high/low) : 105 / 23
Subnet size (first/next) : 24 / 24 (autogrow)
VRF name : abc
Total addresses : 55
Leased addresses : 24
Pending event : none
3 subnets are currently in the pool :
Current index IP address range Leased addresses
25.1.1.12 25.1.1.1 - 25.1.1.14 11
25.1.1.17 25.1.1.17 - 25.1.1.30 0
Interface Ethernet0/1 address assignment
25.1.1.1 255.255.255.248
25.1.1.17 255.255.255.248 secondary
```

The show ip dhcp server statistics command is incorrect because this command is used to view the statistics of the DHCP server.

The show dhcp pool command and show ip dhcp server pool commands are both incorrect because these are not valid Cisco IOS commands.

Objective:

Infrastructure Services

Sub-Objective:

Troubleshoot client- and router-based DHCP connectivity issues

Licensed to Berend Post berend.post@it-university.nl

References:

Question 231

Which of the following fields are in a Transmission Control Protocol (TCP) header? (Choose three.)

- ☐ Length
- ☒ Sequence Number
- ☒ Data Offset
- ☐ Type-of-Service
- ☒ Window

Explanation:

Explanation:

Sequence Number, Data Offset, and Window are the fields found in a TCP header. TCP hosts create a connection-oriented session with one another. The following are the fields found in a TCP header:

Sequence Number: Refers to the first byte of data in the current message. This field helps TCP to reassemble the packets in the correct order. For example, when data is transferred between an FTP server and FTP client, the receiver uses this field to reassemble the packets into the original file.

Data Offset: Refers to the number of 32-bit words in the TCP header.

Window: Refers to the size of the available space for the incoming data.

Source Port and Destination Port: Refer to the point where upper-layer source and destination processes receive TCP services. Both TCP and UDP packets contain these fields.

Acknowledgment Number: Refers to the sequence number of the next byte of data which the sender will receive.

Reserved: Reserved for future use.

Flags: Contains control information, such as the SYN and ACK bits which are used to establish and acknowledge communication, and the FIN bit which is used to terminate the connection.

Checksum: An indicator of any damage to the header while being in transit. Both TCP and UDP packets contain this field.

Urgent Pointer: Refers to the first urgent data byte in the packet.

Options: Used to specify TCP options. Only TCP packets contain this field.

Data: Has upper-layer information.

TCP is used for unicast transmissions and provides connection -oriented services for upper layer protocols. It will establish a state of connection between two devices before any data is transferred; for example, before a workstation can exchange HTTP packets with Web server, a TCP connection must be established between the workstation and the Web server.

 Licensed to Berend Post berend.post@it-university.nl

The Length field is found in a User Datagram Protocol (UDP) header, where it specifies the length of the UDP header and data. UDP headers contain the Source Port, Destination Port, Length, and Checksum fields.

Sequence number, acknowledgment number, and windows size are fields not found in a UDP header because UDP provides none of the services that require use of these fields. That is, UDP cannot re-sequence packets that arrive out of order, nor does UDP acknowledge receipt (thus the term non-guaranteed to describe UDP). Furthermore, since UDP does not acknowledge packets, there is no need to manage the window size, which refers to the number of packets that can be received without an acknowledgment.

The Type-of-Service field is found in an Internet Protocol (IP) header, where it specifies the handling of a current datagram by an upper-layer protocol.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast TCP and UDP protocols

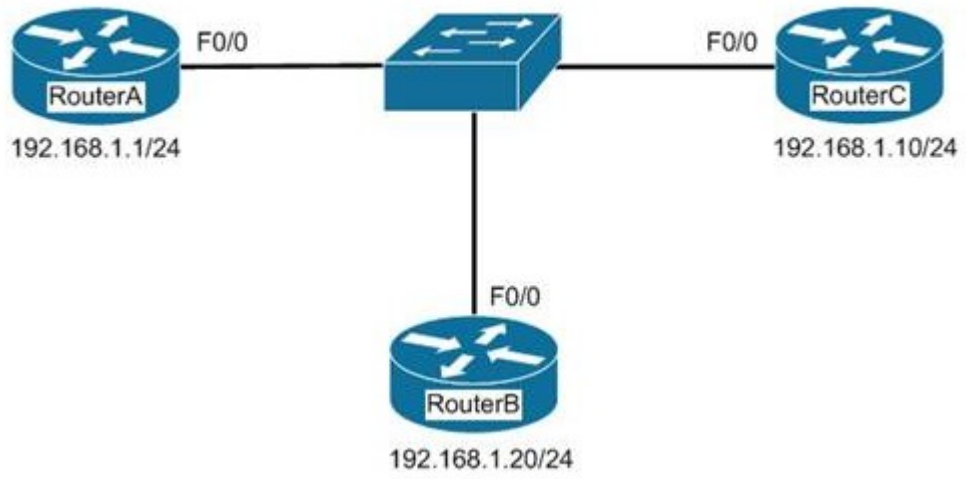
References:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Internet Protocols > TCP Packet Format

Licensed to Berend Post berend.post@it-university.nl

Question 232

In the network exhibit, the routers are running OSPF and are set to the default configurations. (Click the Exhibit(s) button.)



What would be the effect of configuring a loopback interface on RouterA with an address of 192.168.1.50/24?

- ☐ Router B would become the DR
- ☒ Router A would become the DR
- ☐ Router C would become the DR
- ☐ Router A would become the BDR

Explanation:

Explanation:

Configuring a loopback interface on RouterA with an address of 192.168.1.50/24 would cause Router A to become the designated router (DR). The designated router (DR) is determined by the router with the highest interface priority number. If the priority numbers are tied, then the router with the highest router ID (RID) becomes the DR.

The default priority number is 1, and can be configured as high as 255. Changing the priority to 0 would make the router ineligible to become the DR or the backup designated router (BDR). The ip ospf priority # command is used to manually configure a priority on a specific interface.

Router IDs are determined first by the highest loopback IP address, followed by the highest IP address on an active physical interface. Thus, in the case of a priority tie, the router with the highest loopback IP address will have the highest RID, and will become the DR for the network segment.

The current Router ID for a router can be determined by executing the show ip interface brief command. In the sample output of the show ip interface brief command below, the RID will be 10.108.200.5.

Licensed to Berend Post berend.post@it-university.nl

Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol

Ethernet0 10.108.00.5 YES NVRAM up up

Ethernet1 unassigned YES unset administratively down down

Loopback0 10.108.200.5 YES NVRAM up up

Serial0 10.108.100.5 YES NVRAM up up

Serial1 10.108.40.5 YES NVRAM up up

Serial2 10.108.100.5 YES manual up up

Serial3 unassigned YES unset administratively down down

Neither Router B nor C will be the DR because the IP addresses on their physical interfaces are lower than 192.168.1.50/24.

Router A will not be the backup designated router. Since it is the DR, it cannot also be the BDR.

Router C will not be the BDR because its IP address is lower than that of Router B. Router B will be the BDR.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039 > DR Election

Licensed to Berend Post berend.post@it-university.nl

Question 233

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?

- ☒ no cdp run
- ☐ set cdp disable
- ☐ no cdp enable
- ☐ no cdp advertise-v2

Explanation:

Explanation:

You should use the no cdp run command to disable CDP on the router. Due to a known vulnerability regarding the handling of CDP by Cisco routers and switches when devices send large numbers of CDP neighbor announcements, some devices can crash or cause abnormal system behavior. To overcome this problem, you can disable CDP for the entire router by using the no cdp run command.

You cannot use the set cdp disable command to disable CDP on the router. This command disables CDP on an entire Catalyst switch.

You cannot use the no cdp enable command to disable CDP on the router. This command disables CDP on a specific interface.

You cannot use the no cdp advertise-v2 command to disable CDP on the router. This command disables CDPv2 advertisements.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Support > Using Cisco Discovery Protocol

Cisco > Support > Technology Support > Network Management > Cisco's Response to the CDP Issue > Document ID: 13621

Licensed to Berend Post berend.post@it-university.nl

Question 234

Which option lists the given applications in the correct sequence of increasing bandwidth consumption?

- ☒ an interactive Telnet session on a server running an SAP application
- ☒ a voice conversation between PC-based VoIP services
- ☒ a voice conversation between two IP phones while accessing an online video site
- ☐ a voice conversation between two IP phones while accessing an online video site
- ☐ an interactive Telnet session on a server running an SAP application
- ☐ a voice conversation between PC-based VoIP services
- ☐ a voice conversation between PC-based VoIP services
- ☐ a voice conversation between two IP phones while accessing an online video site
- ☐ an interactive Telnet session on a server running an SAP application
- ☐ an interactive Telnet session on a server running an SAP application
- ☐ a voice conversation between two IP phones while accessing an online video site
- ☐ a voice conversation between PC-based VoIP services

Explanation:

Explanation:

The correct sequence of increasing bandwidth consumption in the given scenario would be, from lowest to highest:

an interactive Telnet session on a server running an SAP application

a voice conversation between PC-based VoIP services

a voice conversation between two IP phones while accessing an online video site

An interactive Telnet session uses the least amount of bandwidth of the three application examples because it mainly involves the transfer of text.

A voice conversation between IP phones, also known as voice over IP (VoIP) traffic, requires more bandwidth than Telnet. Voice traffic is delay-sensitive and benefits from Quality of Service (QoS) to ensure service quality.

A voice conversation between two IP phones while accessing an online video site would consume the most bandwidth. A voice conversation with real-time video exchange is the equivalent of real-time video traffic. Video traffic is real-time and benefits from dedicated bandwidth with QoS implementation to ensure quality.

Objective:

WAN Technologies

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Describe basic QoS concepts

References:

Cisco Documentation > Internetworking Technology Handbook > Voice/Data Integration Technologies

Question 235

As part of a new initiative to tighten the security of your Cisco devices, you have configured the firewall to restrict access to the devices from the outside.

What would be other recommended ways of protecting the integrity of the device configuration files on the devices while ensuring your continued ability to manage the devices remotely? (Choose all that apply.)

- ☐ encrypt the configuration files
- ☒ use SSH to connect to the devices for management
- ☐ prevent the loss of administrator passwords by disabling their encryption
- ☐ disable the VTY ports on the devices
- ☒ use an encrypted password for VTY access

Explanation:

Explanation:

You should use SSH to connect to the devices for management. You should also require an encrypted password for VTY access. Using Telnet for remote management transmits all information, including the username and passwords, in clear text. Using an encrypted password for VTY access ensures that the password cannot be read either in transit or in the configuration file.

Passwords used for access to the console, aux, or VTY connections can be encrypted if desired. When passwords are created with the enable <password> command, the password is saved in clear text. When the enable secret <password> command is used, however the password will be encrypted.

If both types of password are configured for a particular connection type, the system will ignore the enable password and require the enable secret password. For example, if the set of commands shown below were executed, both types of password will be created for console access, but the system will require the password crisco rather than cisco. Also make note that neither of those passwords will required for VTY access. That password is sicso, which is the password configured after accessing the line VTY interface configuration prompt.

Router(config)# enable secret crisco

Router(config)# enable password cisco

 Licensed to Berend Post berend.post@it-university.nl

Router(config)# line vty 0 4

Router(config-line)# password sisco

Although it is possible to encrypt the password in the configuration files, it is not possible to encrypt the rest of the files.

You should not disable the encryption of the passwords in the configuration files. Password encryption is a good security measure to take, and sloppy password management should not be a reason to change this practice.

You should not disable the VTY ports on the devices. This would certainly enhance security, but it would prevent you from managing the devices remotely

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco IOS Security Configuration Guide, Release 12.2>Security Overview

Question 236

Which of the following technologies should be used to prevent a switching loop if a switch is connected to a port configured for PortFast?

- ☐ RSTP
- ☒ BPDU Guard
- ☐ Root Guard
- ☐ PVST

Explanation:

Explanation:

BPDU Guard prevents switching loops in the case of a switch being connected to a PortFast interface. PortFast is used for ports that connect to host systems, such as workstations and printers, and allows the port to immediately enter a forwarding state. This bypasses the normal 30-second delay that Spanning Tree Protocol would normally use to determine if a switch has been connected to the port. Implementing BPDU Guard will disable the port if a switch is connected and a BPDU is received.

 Licensed to Berend Post berend.post@it-university.nl

Rapid Spanning Tree Protocol (RSTP) is incorrect because this is an enhanced Spanning Tree standard that operates on the Data Link layer of the OSI model. RSTP was not designed to protect PortFast ports. PortFast and BPDU Guard are supported by RSTP, but they not required or configured by default.

Root Guard is incorrect because it is used to protect the root bridge placement in the Spanning Tree, not to protect PortFast ports.

Per-VLAN Spanning Tree (PVST) is incorrect because this is an implementation of Spanning Tree (the default protocol for Cisco switches), and was not designed to protect PortFast ports. PortFast and BPDU Guard are supported by RSTP, but are not required, and must be configured manually.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP-related optional features

References:

Cisco > Support > Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, and LoopGuard > Understanding How PortFast Works

CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot STP protocols

Question 237

Which Wide Area Network (WAN) switching technology is used by Asynchronous Transfer Mode (ATM)?

- ☐ packet switching
- ☐ virtual switching
- ☐ circuit switching
- ☒ cell switching

Explanation:

Explanation:

Cell switching is a WAN switching technology that is used by ATM. ATM is an International Telecommunication Union-Telecommunications (ITU-T) standard for transmission of data, voice, or video traffic using a fixed size frame of 53 bytes, known as cells. Out of these 53 bytes, the initial five bytes are header information and the rest 48 bytes is the payload.

 Licensed to Berend Post berend.post@it-university.nl

Packet switching is incorrect because packet switching is popularly used for data transfer, as data is not delay sensitive and it does not require real time transfer from a sender to a receiver. With packet switching, the data is broken into labeled packets and transmitted using packet-switching networks.

Virtual switching is incorrect because no such WAN switching technology exists.

Circuit switching is incorrect because circuit switching dynamically establishes a virtual connection between a source and destination. The virtual connection cannot be used by other callers unless the circuit is released. Circuit switching is the most common technique used by the Public Switched Telephone Network (PSTN) to make phone calls. A dedicated circuit is temporarily established for the duration of call between caller and receiver. Once the caller or receiver hangs up the phone, the circuit is released and is available for other users.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies > Circuit Switching

Question 238

If a routing table contains multiple routes for the same destination, which were inserted by the following methods, which route will the router use to reach the destination network?

- ☐ The route inserted by RIP
- ☐ The route inserted by OSPF
- ☐ The route inserted by BGP
- ☒ The route configured as a static route

Explanation:

Explanation:

A static route will be preferred because it has the lowest administrative distance. Routing protocols are dynamic routing methods. With the default configuration, static routes are preferred over dynamic routes.

The default administrative distance for the offered options is:

 Licensed to Berend Post berend.post@it-university.nl

RIP 120

OSPF 110

eBGP 20

Static 1

When Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and static routing is enabled on a router, the router will prefer the static route.

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics

Question 239

What is the term used for the Ethernet communication mechanism by which hosts can send and receive data simultaneously?

- ☒ full-duplex
- ☐ multiplex
- ☐ half-duplex
- ☐ duplex

Explanation:

Explanation:

Full-duplex communication occurs when workstations can send and receive data simultaneously. To support full-duplex communication, both communicating hosts should be configured to transmit in full-duplex mode. With the use of full-duplex communication, the bandwidth can effectively be doubled. Hubs are not capable of handling full-duplex communication, and you need a dedicated switch port to allow full-duplex communication.

Half-duplex is the term used for the Ethernet communication mechanism when hosts can send or receive data, but not simultaneously.

Licensed to Berend Post berend.post@it-university.nl

It is important that the switch and the device connected to the switch have the same duplex and speed settings, or there will intermittent connectivity and loss of connection. To verify the duplex and speed settings on a switch, execute the show interfaces command, specifying the interface and the setting can be verified (as shown in line 8 in the output below):

switch# show interface fastethernet 0/3

Fast Ethernet 0/3 is down, line protocol is down (not connect)

Hardware is Fast Ethernet, address is 00e0.1e3e.2a02

MTU 1500 bytes, BW 10000 Kbit, DLY 100 usec, rely 1/255, tx load

1/255, rxload 1/255

Encapsulation ARPA, loopback not set,

Keepalive set (10 sec)

Half-duplex, 100Mb/s

ARP type: ARPA, ARP Timeout 04:00:00

From the output above it can be seen that the switch interface is set for half duplex and the speed is set for 100Mb/s. This means that if the host connected to this switch port is set differently, for example set to 1 Gb/s because it has a 1 Gb NIC, the host and the switch interface will not communicate and the host will not be able to connect to the network.

Multiplex is the term used when multiple signals are combined to be transferred via one signal.

Duplex implies that there are two communication paths. However, the term does not specify the required functionality, which is full duplex.

Objective:

LAN Switching Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Describe and verify switching concepts

References:

Cisco > Support > Technology Support > LAN Switching > Ethernet > Design > Design Technotes > Configuring and Troubleshooting Ethernet 10/100/1000Mb Half/Full Duplex Auto-Negotiation > Document ID: 10561

Question 240

When transmitting to a remote destination, what two things will occur after a host has determined the IP address of the destination to which it is transmitting? (Choose two.)

- ☐ The sending host will perform an ARP broadcast in its local subnet using the IP address of the destination host.
- ☒ The sending host will perform an ARP broadcast in its local subnet using the IP address of the local router interface.
- ☐ The local router interface will respond with the MAC address of the destination host.
- ☒ The local router interface will respond with its own MAC address.
- ☐ The destination host will respond with its own MAC address.

Explanation:

Explanation:

When a transmission is made to a remote location, the sending host will perform an Address Resolution Protocol (ARP) broadcast in its local subnet using the IP address of the local router interface, and the local router interface will respond with its own MAC address. A remote address is defined as an address in a different subnet.

When a host determines (through a process called ANDing) that a destination address is remote, it will send the packet to the local router interface, which is known as the default gateway on the host. But when it performs ANDing on the IP address of the local router interface, it will discover that the interface is local. When transmitting to a local IP address, a conversion to a MAC address must occur. Therefore, it will perform a local ARP broadcast, and the local router interface will respond with its MAC address.

Regardless of whether the host is broadcasting for the MAC address of the destination locally on the same LAN, or if it is broadcasting for the MAC address of the router interface (remotely), the broadcast will be a Layer 2 broadcast using the MAC address ff-ff-ff-ff-ff. It will be received by all devices on the LAN, but only the device with the specified IP address will reply.

 Licensed to Berend Post berend.post@it-university.nl

The ARP resolution process does take a second or two to complete if no mapping for the destination devices IP address to MAC address is found in the ARP cache. For example, if the MAC address must be resolved through the ARP broadcast when pinging from one device to another, it can cause the first several echo requests to go unanswered, as shown on the output below. After this resolution has been completed, however, the second ping attempt should receive an answer to all five ICMP echo requests.

Router1#ping 50.6.3.26

Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 50.6.3.26, timeout is 2 seconds:

..!!!

Router1#ping 50.6.3.26

Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 50.6.3.26, timeout is 2 seconds:

!!!!!

The sending host will not perform an ARP broadcast in its local subnet using the IP address of the destination host. A local ARP broadcast is only performed when the ANDing process deduces that the destination IP address is local. In this case, the destination is remote.

The destination host will not respond with its MAC address. The process of learning the MAC address of the destination computer is the responsibility of the local router interface on the subnet where the destination host resides.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Cisco > Cisco IOS XR IP Addresses and Services Configuration Guide for the Cisco XR 12000 Series Router, Release 4.3.x > Configuring ARP

 Licensed to Berend Post berend.post@it-university.nl

Question 241

You just finished configuring VLAN Trunking Protocol (VTP) in a network containing five switches. One of the switches is not receiving VLAN information from the switch that is acting as the server.

Which of the following could NOT be a reason why the switch is not receiving the information?

- ☐ The VTP domain name on the switch may be misspelled
- ☐ The VTP password may be misspelled on the switch
- ☒ The configuration revision number may be out of sync
- ☐ The VTP version used on the switch may be different

Explanation:

Explanation:

The configuration revision number does not need to match on the switches. The configuration number cannot be directly configured, but is instead synchronized during VTP updates.

For VTP to function correctly, all of the following conditions must be true:

The VTP version must be the same on all switches in a VTP domain.

The VTP password must be the same on all switches in a VTP domain.

The VTP domain name must be the same on all switches in a VTP domain.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

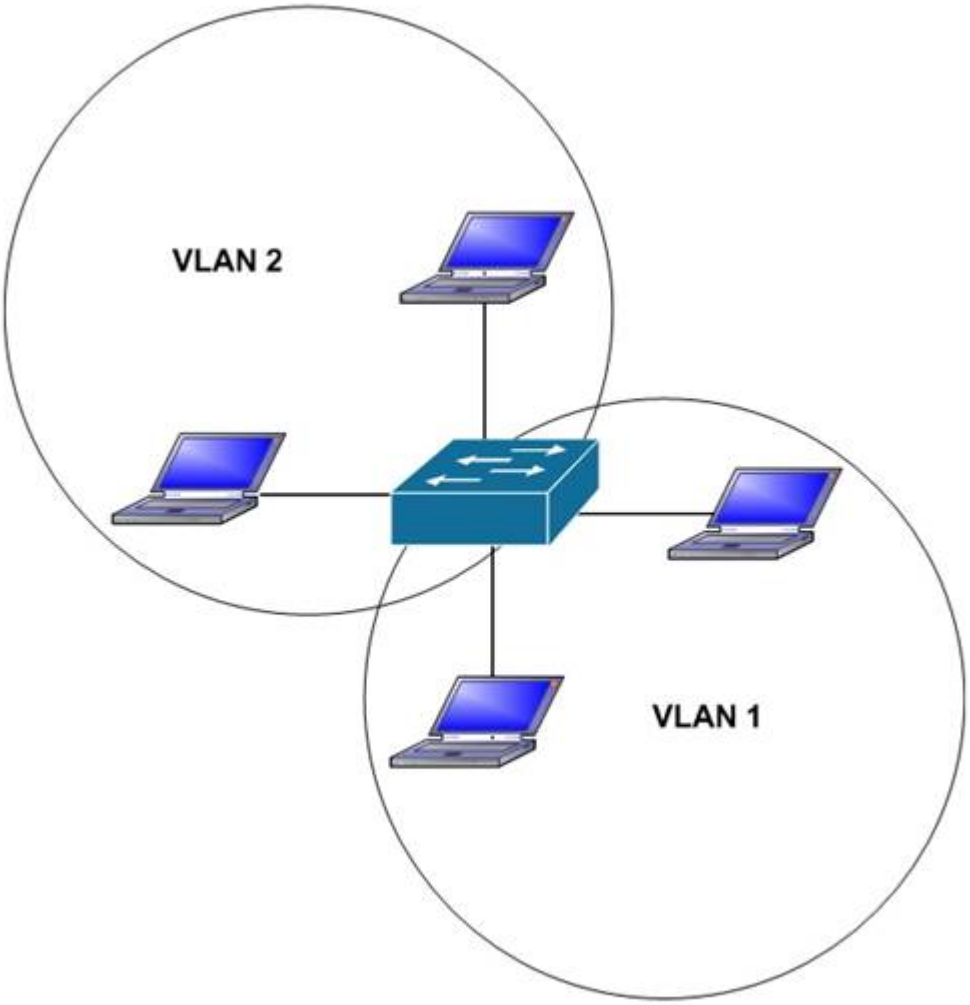
References:

CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot STP protocols

Licensed to Berend Post berend.post@it-university.nl

Question 242

Which of the following statements are true with regard to the network shown in the exhibit? (Click the Exhibit(s) button.)



- ☐ there is one broadcast domain and one collision domain
- ☐ there is one broadcast domain and four collision domains
- ☐ there are two broadcast domains and two collision domains
- ☒ there are two broadcast domains and four collision domains
- ☒ the hosts in VLAN1 could use IP addresses 192.168.5.4/24 and 192.168.5.5/24 and the hosts in VLAN2 could use IP addresses 192.168.6.1/24 and 192.168.6.2/24
- ☐ the hosts in VLAN2 could use IP addresses 192.168.5.5/24 and 192.168.6.5/24

Explanation:

Explanation:

There are two broadcast domains and four collision domains in the network shown in exhibit. A Virtual LAN (VLAN) is a group of networking devices in the same broadcast domain. A broadcast domain is a group of devices such that when one device in the group sends a broadcast, all the other

Licensed to Berend Post berend.post@it-university.nl

devices in the group will receive that broadcast. Because there are two VLANs shown in the exhibit, VLAN1 and VLAN2, there are two broadcast domains. A switch will not forward broadcast frames between VLANs.

A collision domain is a domain where two or more devices in the domain could cause a collision by sending frames at the same time. Each switch port is a separate collision domain. Because there are four switch ports in the exhibit, there are four collision domains.

The hosts in VLAN1 could use IP addresses 192.168.5.4/24 and 192.168.5.5/24 and the hosts in VLAN2 could use IP addresses 192.168.6.1/24 and 192.168.6.2/24. Hosts in different VLANs must have IP addresses that are in different subnets.

The other options that offer IP address plans are incorrect because they either place hosts from different VLANs in the same subnet, or place hosts in the same VLAN in different subnets.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Cisco > Support>Technology Support > LAN Switching > Layer-Three-Switching and Forwarding > Configure > Configuration Examples and TechNotes > How To Configure InterVLAN Routing on Layer 3 Switches

Question 243

Which command will save a dynamically learned MAC address in the running-configuration of a Cisco switch?

- ☐ switchport port-security mac-address
- ☐ switchport port-security
- ☐ switchport port-security sticky mac-address
- ☒ switchport port-security mac-address sticky
- ☐ switchport mac-address sticky

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Issuing the switchport port-security mac-address sticky command will allow a switch to save a dynamically learned MAC address in the running-configuration of the switch, which prevents the administrator from having to document or configure specific MAC addresses. Once the approved MAC addresses have all been learned, the network administrator simply saves the running-configuration file to NVRAM with the copy running-config startup-config command.

Switches dynamically build MAC address tables in RAM, which allow the switch to forward incoming frames to the correct target port. By default, an unlimited number of MAC addresses can be learned on a single switch port, whether it is configured as an access port or a trunk port. Switch ports can be secured by defining one or more specific MAC addresses that should be allowed to connect, and by defining violation policies (such as disabling the port) if additional hosts try to gain a connection. The following command secures a switch by manually defining an allowed MAC address:

switch(config-if)# switchport port-security mac-address 00C0.35F0.8301

This command statically defines the MAC address of 00c0.35F0.8301 as an allowed host on the switch port. Manually configuring all of your switch ports in this way, however, would require documenting all of your existing MAC addresses and configuring them specifically per switch port, which could be an extremely time-consuming task.

An example of the use of the switchport port-security mac-address sticky command is shown below:

Switch(config)#interface fastethernet0/16

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security maximum 1

With the above configuration, if a computer with a MAC address of 0000.00bb.bbbb were plugged into the switch, the following two things would occur:

Only the host with MAC address 000.00bb.bbbb will be allowed to transmit on the port. This is a result of the port-security mac-address-sticky command, which instructs the switch to learn the next MAC address it sees on the port, and of the port-security maximum 1 command, which further instructs the switch that the address learned is the only address allowed on the port.

All frames arriving at the switch with a destination address of 0000.00bb.bbb will be forwarded out on Fa0/16.

Licensed to Berend Post berend.post@it-university.nl

The switchport port-security mac-address sticky command can also be used in combination with the interface-range command to make every port on the switch behave in this fashion as shown below for a 24-port switch.

Switch(config)#interface range fastethernet0/1-24

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security maximum 1

The switchport port-security mac-address command is incorrect since this command requires an additional argument to be valid (either a statically configured MAC address or the sticky option).

The switchport port-security command activates port security on the switch port, but does not configure sticky MAC address learning.

The switchport port-security sticky mac-address and switchport mac-address sticky options are incorrect because these are not valid Cisco IOS commands.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

Cisco > Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide > Configuring Port Security > Enabling Port Security with Sticky MAC Addresses on a Port

Cisco > Cisco IOS Security Command Reference > show vtemplate through switchport port-security violation > switchport port-security mac-address

Licensed to Berend Post berend.post@it-university.nl

Question 244

Which of the following is NOT a possible component of Enhanced Interior Gateway Routing Protocol's (EIGRP) composite metric?

- ☒ Cost
- ☐ Load
- ☐ Delay
- ☐ Bandwidth

Explanation:

Explanation:

Cost is not a component of EIGRP's composite metric. The cost, or efficiency, of a path is used as a metric by the Open Shortest Path First (OSPF) routing protocol.

Enhanced IGRP (EIGRP) is Cisco Systems' proprietary routing protocol. It can use bandwidth, delay, load, reliability, and maximum transmission unit (MTU) to calculate the metric. Of these five metrics, by default, only minimum bandwidth and delay are used to compute the best path.

The metric for EIGRP can be calculated with this formula:

Metric = [K1 * Bandwidth + (K2 * Bandwidth) / (256-load) + K3*Delay] * [K5 / (reliability + K4)]

The default constant values for Cisco routers are K1 = 1, K3 = 1, and K2 = 0, K4 = 0, K5 = 0. In the default setting, K1 and K3 have non-zero values, and therefore, by default, the metric is dependent on bandwidth and delay.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Support > IP > IP Routing > Design > Design TechNotes > Introduction to EIGRP > Document ID: 13669

Licensed to Berend Post berend.post@it-university.nl

Question 245

A new trainee is setting up a router in a test lab, and he asks you to describe the use of the connector marked BRI on the router.

Which is a correct use for this connecter?

- ☐ A WAN interface for a T1 connection
- ☐ A LAN interface to connect to a switch
- ☐ An interface to connect a console cable
- ☒ A WAN interface for an ISDN connection

Explanation:

Explanation:

The connector marked BRI is used for an Integrated Services Digital Network (ISDN) connection, specifically a basic rate interface (BRI). An ISDN basic rate interface provides three channels: a D channel for control signaling, and two B or bearer channels for data, resulting in 128 bits of bandwidth.

A WAN interface for a T1 connection would be connected to a serial port on the router, not the BRI interface. It would not accept a basic rate ISDN connection.

A LAN interface to connect to a switch would be an Ethernet connection that used either an RJ-45 connector or a legacy AUI connector. It would not accept a basic rate ISDN connection

An interface to a console connector will look like an RJ-45 Ethernet connector but will only accept a console or rollover cable, and is used to manage the router. It would not accept a basic rate ISDN connection.

These various ports can be seen on the backplane of a router as shown below:



Objective:

WAN Technologies

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Describe WAN access connectivity options

References:

http://www.tutorialsweb.com/networking/routers/cisco-rotuers-ios.htm#Hardware%20Components:

Cisco>Support>Product Support>End-of-Sale and End-of-Life Products>Cisco 3600 Series Multiservice Platforms>Troubleshoot and Alerts> Troubleshooting TechNotes> Understanding the 1-Port ISDN BRI (S/T) WAN Interface Card (WIC-1B-S/T or WIC36-1B-S/T)

Question 246

You instructed your assistant to add a new router to the network. The routers in your network run OSPF. The existing router, OldRouter, is configured as follows:

router ospf 1
network 192.168.5.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0

The OldRouter interface that connects to NewRouter is 192.168.5.3/24. Your assistant shows you the configuration that will be implemented:

newrouter(config)# router ospf 1
newrouter(config-router)# network 192.168.5.0 255.255.255.0 area 0

What is wrong with this configuration?

- ☐ The area ID is incorrectly configured.
- ☒ The wildcard mask is incorrectly configured.
- ☐ The network statement is incorrectly configured.
- ☐ The process ID number is incorrectly configured.

Explanation:

Explanation:

When entering network statements for OSPF, a wildcard mask is used instead of a regular mask. Since the network connecting the two routers is a class C network, as shown by the address 192.168.5.0/24, the wildcard mask should be 0.0.0.255 rather than 255.255.255.0. With wildcard masks, the 0s octets must match, and the 255s octets do not have to match.

The area ID is correct. OldRouter is in area 0, so NewRouter should be as well. There must be an area 0 in an OSPF network. There can be multiple areas as well, but they must all connect to area 0. If non-0 areas cannot be directly connected to area 0, they must be configured with a virtual link across an area that does connect to the backbone (area 0).

 Licensed to Berend Post berend.post@it-university.nl

The network statement is correct. The network between the routers is 192.168.5.0.

The process ID number is correct. The number is stated as OSPF 1 on OldRouter and OSPF 1 on NewRouter. They match in this case but that is not required. Process IDs are only locally significant.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Internetworking Technology Handbook > Open Shortest Path First (OSPF)

Question 247

You are discovering that there are differences between the configuration of EIGRP for IPv6 and EIGRP for IPv4. Which statement is true with regard to the difference?

- ☒ A router ID is required for both versions
- ☐ A router ID must be configured under the routing process for EIGRP for IPv4
- ☐ AS numbers are not required in EIGRP for IPv6
- ☐ AS numbers are not required in EIGRP for IPv4

Explanation:

Explanation:

Both versions of EIGRP require a router ID. The difference is that with EIGRP for IPv6, you must configure a router ID under the routing process if there are no IPv4 addresses on the router. In EIGRP for IPv4, the router can select one of the configured IPv4 addresses as the router ID.

A router ID can be configured under the routing process for EIGRP for IPv4, but it is not required. In EIGRP for IPv4, the router can select one of the configured Pv4 addresses as the router ID.

AS numbers are required in both versions of EIGRP.

Objective:

Routing Fundamentals

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Home > Articles > Cisco Certification > CCNA Routing and Switching > C > Cisco ICND2 Foundation Learning Guide: Implementing an EIGRP Solution > Implementing EIGRP for IPv6

Question 248

Which command will display the Virtual LAN (VLAN) frame tagging method for a switch link?

- ☐ show vlan
- ☐ show vlan encapsulation
- ☐ show vtp status
- ☒ show interfaces trunk

Explanation:

Explanation:

The show interfaces trunk command displays the list of trunk ports and the configured VLAN frame tagging methods.

Sample output of the show interfaces trunk command would be as follows:

SwitchB# show interfaces trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Fa0/2 on 802.1q trunking 1

Fa0/3 on 802.1q trunking 1

<<output omitted>>

The show vlan command displays the VLAN number, name, status, and ports assigned to individual VLANs. Although the command cannot be used to determine the frame tagging method used for each trunk, it can be used to determine which ports are trunk ports by the process of elimination.

In the output below, generated from a six-port switch, the missing port (Fa0/6) is a trunk port. For communication to be possible between the two VLANs configured on the switch, Fa0/6 must be connected to a router, and trunking must be configured on the router end as well. The command is

 Licensed to Berend Post berend.post@it-university.nl

also useful for verifying that a port has been assigned to the correct VLAN as it indicates in the VLAN column the VLAN to which each port belongs.

Switch# show vlan

Vlan	name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
58	vlan 58	active	Fa0/5

The show vlan encapsulation command is not a valid command for Cisco switches.

The show vtp status command does not display VLAN frame tagging method. The command is used to verify the status of VTP. The output of the show vtp status command would be as follows:

```
SwitchB# show vtp status
VTP Version : 2
Configuration Revision : 1
Maximum VLANs supported locally : 64
Number of existing VLANs : 16
VTP Operating Mode : Client
VTP Domain Name : MARKETING
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x4D 0x60 0xA3 0x5E 0xC7 0x41 0x8C 0x47
```

Line 6 of the given output indicates that the switch is operating in VTP Client mode. There are three possible VTP modes in which a switch can operate: Server, Client, and Transparent.

In Server mode, any changes made in the switch, such as adding a VLAN, will be recorded in the local database and also passed on to the other switches, where the change will be added.

In Client mode, the switch will accept and record changes from switches in Server mode, but will not accept changes made on the local switch.

In Transparent mode, the switch adds changes made locally to the database, but will not send or accept changes sent from other switches.

Licensed to Berend Post berend.post@it-university.nl

The mode in use could be a useful piece of information during troubleshooting. For example, if you were unsuccessfully attempting to add a VLAN to the database, the reason would be that the switch is in VTP Client mode. If you were adding a VLAN in Transparent mode, the VLAN would be added to the local database but fail to appear on the other switches. If the switch were in Transparent mode, Line 6 in the above output would appear as follows:

VTP Operating Mode: Transparent

Only switches operating in VTP Server mode can accept changes to the VLAN database. This situation could be corrected easily and a VLAN 50 could be successfully added at two different configuration prompts by executing the following commands:

At global configuration mode:

switchB# config t

switchB(config)# vtp mode server

switchB(config)# vlan 50

At VLAN configuration mode:

switchB# vlan database

switchB(vlan)# vtp server

switchB(vlan)# vlan 50

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Cisco Press Home > Articles > Cisco Certification > CCNA > CCNA Self-Study (ICND Exam): Extending Switched Networks with Virtual LANs

Licensed to Berend Post berend.post@it-university.nl

Question 249

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.)

- ☒ Ensure the switch is powered up.
- ☐ Reinstall Windows on the workstation.
- ☒ Reseat the cable.
- ☒ Ensure that the cable is straight-through.
- ☐ Ensure that the cable is crossover.

Explanation:

Explanation:

A black or unlit switch port LED is symptomatic of a Layer 1 problem. The port LED should first turn amber and then turn solid green when a host is powered up. The amount of time it takes to turn solid green will depend on the Spanning Tree Protocol configuration. If the LED is unlit, you should ensure that the switch is powered up and that a straight-through cable is used to connect a switch port to a host, such as a workstation or a printer. If the switch is powered up and a straight-through cable is used, reseat the cable to ensure a firm connection.

Reinstalling Windows on the workstation will not help because this is a Layer 1 problem having to do with the switch having power or the use of proper cabling.

You should not ensure that the cable is crossover, because straight-through (patch) cables are used to connect switch ports to hosts.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

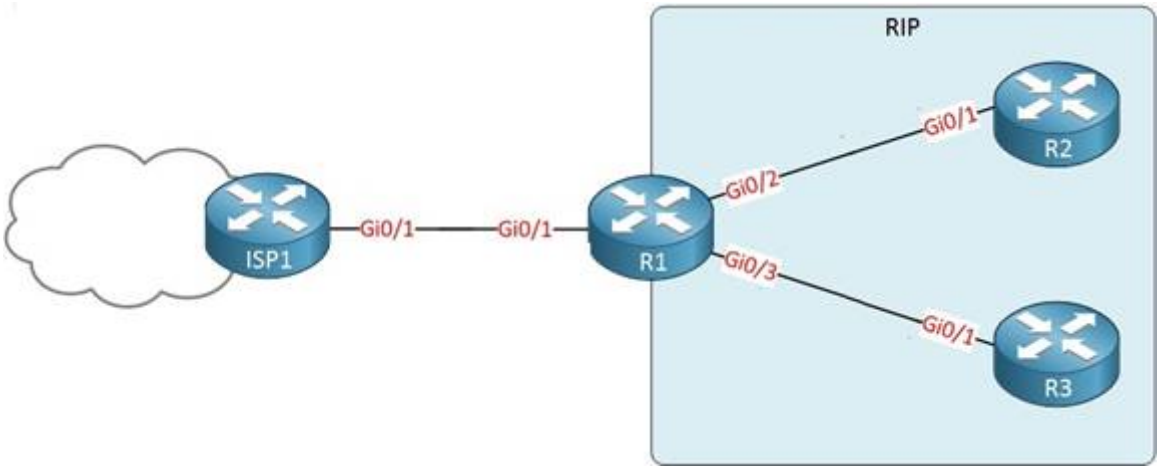
References:

Cisco > Catalyst 2960 Switch Hardware Installation Guide > LEDs

Licensed to Berend Post berend.post@it-university.nl

Question 250

Your network is configured as shown in the following exhibit. When you trace traffic sourced from R3 destined for a LAN network off of R2 (not shown in the diagram), you see the traffic is being forwarded from R1 to ISP1 rather than to R2.



Which of the following issues could NOT be causing this behavior?

- ☐ The network command has not been executed on the interface leading to the LAN off R2
- ☒ The passive interface command has been issued on the Gi0/4 interface of R1
- ☐ A default route exists on R1 that leads to ISP1
- ☐ RIPv2 has not been enabled on R2

Explanation:

Explanation:

This issue would NOT be caused by executing the passive interface command on the Gi0/4 interface of R1. This command prevents the advertisement of RIP routes on that interface. If that command had been issued, the traffic would not be forwarded to R1 because R3 would not know about the route to the LAN off of R2. This command would also prevent R3 from knowing about the default route to ISP1. Since the traffic is being routed to ISP1, this command must not have been executed.

All of the other options could potentially because traffic destined for R2 to be forwarded from R1 to ISP1, rather than to R2.

It is true that a default route exists on R1 that leads to ISP1. If this default route did not exist, the traffic destined for R2 would simply be dropped at R1 instead of being forwarded to ISP1.

If the network command has not been executed on the interface leading to the LAN off of R2, the network leading to the LAN off R2 would not advertised by R2. That would make R1 unaware of this destination. In that case, R1 would use the default route to send traffic destined for R2 to ISP1. We know such a default route must exist, or the traffic would simply be dropped at R1.

Licensed to Berend Post berend.post@it-university.nl

If RIPv2 has not been enabled on R2, R2 would not be receiving or advertising any RIP routes. When the packets destined for the network off of R2 arrive at R1, R1 will have not have a route to that network. In that case R1 will forward the traffic to ISP1 using the default route.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)

References:

Cisco > Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > How Does the Passive Interface Feature Work in EIGRP?

Networkers-Online > Routing > IGP > EIGRP > Passive-interface command behavior in RIP, EIGRP & OSPF

Question 251

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?

- ☒ no cdp run
- ☐ set cdp disable
- ☐ no cdp enable
- ☐ no cdp advertise-v2

Explanation:

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.

 Licensed to Berend Post berend.post@it-university.nl

You cannot use the no cdp enable command to disable CDP on the router. This command disables CDP on a specific interface.

You cannot use the no cdp advertise-v2 command to disable CDP on the router. This command disables CDPv2 advertisements.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Support > Using Cisco Discovery Protocol

Cisco > Support > Technology Support > Network Management > Cisco's Response to the CDP Issue > Document ID: 13621

Question 252

Which Cisco IOS command is used to provide a description to an interface?

- ☒ description
- ☐ interface-description
- ☐ interface description
- ☐ description interface number

Explanation:

Explanation:

The description command is used to provide a description to an interface. It is not a mandatory configuration. However, if you have configured the description for an interface, anyone who is working on the router can easily identify the purpose of the interface. Following is an example of the description command:

RouterA(config)# interface s0

RouterA(config-if)# description AT&T T1 to Internet

All the other options are syntactically incorrect.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

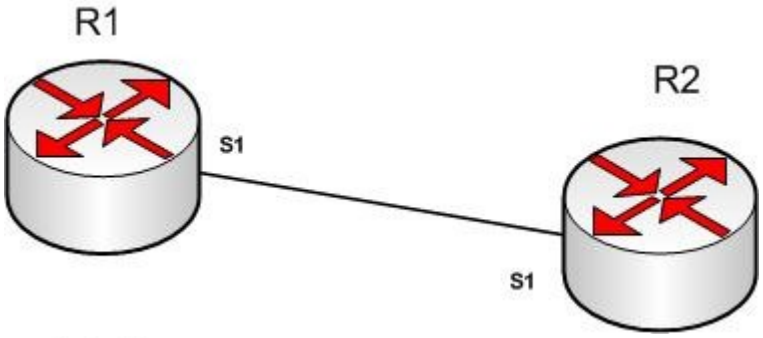
Cisco > Cisco IOS Voice Command Reference > description

Tech Republic > Articles > Cisco administration 101: Five interface commands you should know

Licensed to Berend Post berend.post@it-university.nl

Question 253

R1 and R2 are connected as shown in the diagram and are configured as shown in output in the partial output of the show run command.




```
R1#show run

version 12.0
hostname R1

interface s1
ip address 192.168.5.5 255.255.255.252

ip host R1 192.168.5.6

R2#show run

version 12.0
hostname R2
interface s1
ip address 192.168.5.6 255.255.255.252
ip host R1 192.168.5.5
```

The command ping R2 fails when executed from R1. What command(s) would allow R1 to ping R2 by name?

- ☐ R1(config)#int S1
- ☐ R1(config-if)#no ip address 192.168.5.5
- ☐ R1(config-if)# ip address 192.168.5.9 255.255.255.252
- ☒ R1(config)#no ip host R1
- ☒ R1(config)# ip host R2 192.168.5.6 255.255.255.252
- ☐ R1(config)#no hostname R2
- ☐ R1(config)# hostname R1
- ☐ R2(config)#int S1
- ☐ R1(config-if)#no ip address 192.168.5.5

Licensed to Berend Post berend.post@it-university.nl

- ☐ R1(config-if)# ip address 192.168.5.9 255.255.255.0

Explanation:

Explanation:

Both routers have been configured with the ip host command. This command creates a name to IP address mapping, thereby enabling the pinging of the device by address. On R1, the mapping is incorrect and needs to be corrected. Currently it is configured as ip host R1 192.168.5.6. It is currently mapping its own name to the IP address of R2.

To fix the problem, you should remove the incorrect IP address mapping and create the correct mapping for R2, as follows:

R1(config)#no ip host R1

R1(config)# ip host R2 192.168.5.6 255.255.255.252

Once this is done, the ping on R2 will succeed.

The IP address of the S1 interface on R1 does not need to be changed to 192.168.5.9 /30. In fact, if that is done the S1 interface on R1 and the S1 interface in R2 will no longer be in the same network. With a 30-bit mask configured, the network they are currently in extends from 192.168.5.4 - 192.168.5.7. They are currently set to the two usable addresses in that network, 192.168.5.5 and 192.168.5.6.

The hostnames of the two routers do need to be set correctly using the hostname command for the ping to function, but they are correct now and do not need to be changed.

The subnet mask of the S1 interface on R2 does not need to be changed to 255.255.255.0. The mask needs to match that of R1, which is 255.255.255.252.

Objective:

Infrastructure Services

Sub-Objective:

Troubleshoot client connectivity issues involving DNS

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services, Release 12.3>IP Addressing and Services Commands: idle through ip local-proxy-arp>ip host

Question 254

Which two are NOT valid Cisco IOS commands used for Cisco Discovery Protocol (CDP)? (Choose two.)

- ☐ show cdp
- ☐ show cdp entry *
- ☒ show cdp neighbor entries
- ☐ show cdp neighbors detail
- ☒ show cdp devices

Explanation:

Explanation:

The show cdp neighbor entries command and the show cdp devices command are not valid Cisco IOS commands.

The Cisco IOS commands used for CDP are as follows:

show cdp: This command is used to view global CDP information, such as timer and hold time.

show cdp entry *: This command is used to view information regarding all neighboring devices.

show cdp neighbors detail: This command is used to view the details regarding the neighboring devices which are discovered by the CDP. This command is used to view details such as network address, enabled protocols, and hold time. The complete syntax of this command is:

show cdp neighbors [type number] [detail]

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Cisco IOS Network Command Reference, Release 12.4 > show cdp neighbors

Licensed to Berend Post berend.post@it-university.nl

Question 255

You are configuring a serial link between a Cisco router and a router produced by another vendor. What would be the advantages of using Point to Point Protocol (PPP) over High Level Data Link Control (HDLC) in this scenario?

- ☒ HDLC has a proprietary "type" field that may be incompatible with equipment from other vendors.
- ☐ HDLC is not available on non-Cisco routers.
- ☐ PPP is faster.
- ☐ PPP performs error checking.

Explanation:

Explanation:

High Level Data Link Control (HDLC) has a proprietary "type" field that may be incompatible with equipment from other vendors. It is recommended that PPP always be used when combining equipment from multiple vendors because this Data Link layer WAN protocol is an industry standard. PPP is implemented in the same manner on all PPP-capable equipment.

HDLC is available on non-Cisco routers. However, the Cisco implementation has a "type" field that may prevent the connection from working.

PPP is not faster than HDLC.

PPP performs error checking, but so does HDLC.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco > Internetworking Technology Handbook > Point to Point Protocol (PPP)

Licensed to Berend Post berend.post@it-university.nl

Question 256

Which of the following protocols allow the root switch location to be optimized per VLAN? (Choose all that apply.)

- ☒ PVST+
- ☐ RSTP
- ☒ PVRST
- ☐ STP

Explanation:

Explanation:

Both Per VLAN Spanning Tree Plus (PVST+) and Per VLAN Rapid Spanning Tree (PVRST) protocols allow for a spanning tree instance for each VLAN, allowing for the location optimization of the root bridge for each VLAN. These are Cisco proprietary enhancements to the 802.1d and 802.1w standards, respectively.

Rapid Spanning Tree Protocol (RSTP) is another name for the 802.1w standard. It supports only one instance of spanning tree.

Spanning Tree Protocol (STP) is another name for the 802.1d standard. It supports only one instance of spanning tree.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco Home > Support > Technology Support > LAN Switching

Question 257

Which command is used on the Cisco Catalyst 2950 series switch to configure a port as a VLAN trunk port?

- ☒ switchport mode trunk
- ☐ set trunk on
- ☐ switchport trunk on
- ☐ trunk mode on

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The switchport mode trunk command is used on the Cisco Catalyst 2950 switch to configure a port as a VLAN trunk port. The syntax of the command is as follows:

Switch(config-if)# switchport mode trunk

Trunk links are required between devices in any situation where traffic from multiple VLANs will traverse the link. This is also true when using VTP on the switches and in that case, even if inter-VLAN routing is not required. For example, if two switches in a VTP domain are connected together via an access link with no router present, then when you create a new VLAN on one of the switches, it will NOT be learned by the other switch.

When you configure a trunk link, there are two choices for encapsulation: 802.1q, which is the industry standard, and ISL, which is Cisco proprietary and will only work when both ends are Cisco equipment. Both protocols perform a crucial role in inter-VLAN routing by tagging packets with the VLAN to which the packets belong.

The following commands should be issued to configure FastEthernet 0/1 to function as a VLAN trunk port and use 802.1q encapsulation:

Switch# configure terminal

Switch(config)# interface fastethernet 0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

When configuring a trunk link between a switch and switch, the above commands would be used in both switches. However, when a trunk link is configured between a router and a switch, the process is different on the router. On the router end, you must do the following:

1. Enable the physical interface hosting the trunk link.

2. Ensure that no IP address exists on the physical interface.

3. Create a subinterface for each VLAN on the physical interface.

4. Set the trunking protocol on each subinterface.

5. Configure an IP address on each subinterface.

 Licensed to Berend Post berend.post@it-university.nl

The command set that would create a subinterface for VLAN 10, set the trunking protocol for the subinterface, and assign the subinterface an IP address is:

Router(config)#interface fastethernet 0/0

Router(config)#no ip address

Router(config-if)#no shutdown

Router(config)-if)exit

Router(config)#interface fastethernet 0/0.1

Router(config-if)#encapsulation dot1q 10

Router(config-if)#ip address 192.168.5.1 255.255.255.0

The set trunk on, switchport trunk on , and trunk mode on commands are incorrect because these are not valid Cisco IOS commands.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Cisco Catalyst 2950 Desktop Switch Software Configuration Guide, 12.0(5.2)WC(1) > Creating and Maintaining VLANs > CLI: Configuring a Trunk Port

Cisco > Cisco IOS Interface and Hardware Component Command Reference >squelch through system jumbomtu > switchport mode

Question 258

What command would you run to determine which switch is the root bridge for a particular VLAN?

- ☐ show spantree vlan
- ☐ show spanning tree
- ☐ show vlan spantree
- ☒ show spanning-tree vlan
- ☐ show spanning-tree interface

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The show spanning-tree vlan command provides Spanning Tree Protocol (STP) information on the root switch, including the bridge ID, root path, and root cost, as well as information on the local switch. The output of the command is as follows:

```
Switch# show spanning-tree vlan 1
VLAN0001

Spanning tree enabled protocol ieee
Root ID      Priority      0
Address      000c.00d3.5124
Cost           19
Port           2 (FastEthernet0/2)
Hello Time      2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000c.14f5.b5c0
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface      Role      Sts      Cost      Prio.Nbr      Type
--------- ---- --- ---- -------- --------------
Fa0/2      Root      FWD      19      128.2      P2p
Fa0/10      Desg      FWD      19      128.10      P2p
Fa0/1      Altn      BLK      19      128.1      P2p
```

This output indicates the following:

The root switch has a bridge ID (Priority + MAC Address) of 0-000c.00d3.5124, while the local switch has a bridge ID of 32769-000c.14f5.b5c0. This indicates that the local switch is not the root switch for VLAN 1. Additional evidence that the local switch is not the root switch is the fact that the Fa0/1 port is blocking with a role listed as Altn. Only non- root bridges have blocking ports.

For this switch, Fa0/1 represents the redundant link that needs to be blocked to prevent a switching loop.

Interface Fa0/2 is the root port (the interface with the shortest path to the root switch).

All three links have a cost of 19, which is the default cost of a single FastEthernet link.

802.1d is enabled in this switch, as indicated by the output Spanning tree enabled protocol ieee in line 2.

The show spanning-tree interface command will indicate the port role and state that a particular interface plays in each VLAN, but does not indicate the root bridge for a particular VLAN. Below is sample output from the show spanning-tree interface fastethernet0/1 command. In this example, RSTP is in use rather than 802.1d.

Licensed to Berend Post berend.post@it-university.nl

```
Switch# show spanning-tree interface fastethernet0/1

VLAN          Role          Sts Cost          Prior.Nbr Type
--------------------------------------------------------------------------
VLAN0001      Altn          BLK     19          128.2          P2P
VLAN0002      Root          FWD     19          128.1          P2P
VLAN0003      Root          FWD     19          128.1          P2P
```

In the above output, the Fa0/1 interface is not the root bridge for any of the three VLANs. It is the root port for VLANs 2 and 3. Root bridges have only designated ports. It is the alternate port for VLAN1, which means that Fa0/1 has a higher cost path to the root bridge than another interface in the topology, and will be in a blocking state as long as that other path is available.

The other options are incorrect because they are not valid Cisco IOS commands. The correct syntax would be show spanning-tree, not show spanning tree or show spantree.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Cisco IOS Switching Command Reference > show spanning-tree

Question 259

You are working with an Internet Service Provider (ISP) as network manager. A corporate client approaches you to lease a public IP subnet that can accommodate 250 users. You have assigned him the 192.25.27.0 subnet.

What subnet mask should be assigned to this IP address so that it can accommodate the number of users required by the corporate client?

- ☒ 255.255.255.0
- ☐ 255.255.255.128
- ☐ 255.255.255.224
- ☐ 255.255.255.252

Explanation:

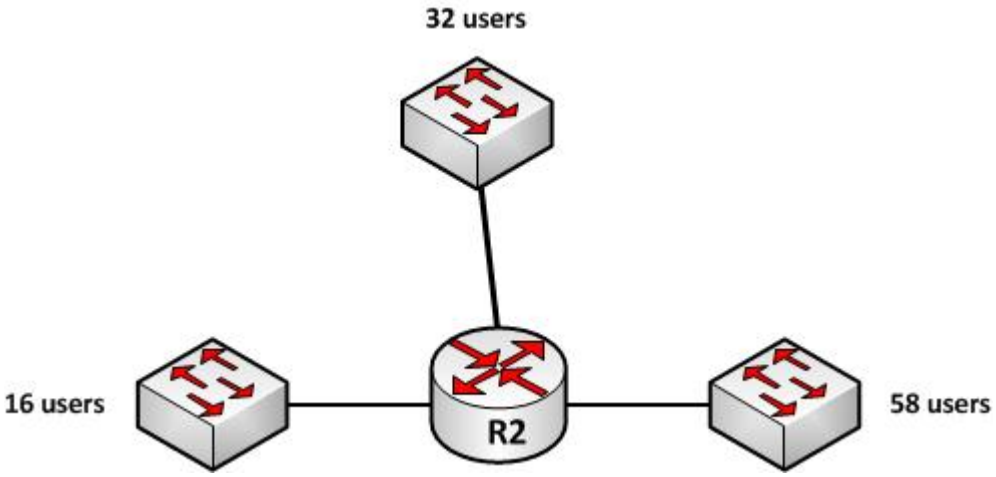
Explanation:

The 192.25.27.0 subnet should be assigned the subnet mask of 255.255.255.0 to accommodate 250 users. This subnet mask can accommodate a maximum of 254 hosts. The number of hosts that can

Licensed to Berend Post berend.post@it-university.nl

reside on a subnet can be calculated using the formula 2n - 2 = x, where n is equal to the number of hosts bits in the mask and x is the resulting number of hosts. 2 is subtracted from the results to represent the two address, the network ID and the broadcast address, that cannot be assigned to computers in the subnet. Since the 255.255.255.0 mask leaves 8 bits at the end of the mask, the formula will be 28 - 2, which is 256 - 2, which equals 254.

In situations where the same subnet mask must be used for multiple interfaces on a router, the subnet mask that is chosen must provide capacity sufficient for the largest number of hosts on any single interface while also providing the required number of subnets. For example, in the diagram below, the three interfaces on the router R2 have 16, 32 and 58 users respectively on each interface:



If each interface must have the same subnet mask, the subnet mask would need to be one that yields at least 58 addresses to support the interface with the highest host count and yields at least 3 subnets as well.

If the chosen classful networks were 128.107.4.0/24, the correct mask would be 255.255.255.192. Since the mask is currently 255.255.255.0 (/24), by borrowing 2 bits to /26 or 255.255.255.192, we will get 4 subnets (22 = 4) and each subnet will yield 62 hosts (26 - 2 = 62).

With a subnet mask of 255.255.255.128, the 192.25.27.0 subnet can accommodate only 126 hosts. The mask 255.255.255.128 leaves 7 host bits in the mask and when we plug that into the formula we get 27 - 2, which equals 126.

With a subnet mask of 255.255.255.224, the 192.25.27.0 subnet can accommodate only 30 hosts. The mask 255.255.255.224 leaves 5 host bits in the mask and when we plug that into the formula we get 25 - 2, which equals 30.

Licensed to Berend Post berend.post@it-university.nl

With a subnet mask of 255.255.255.252, the IP address 192.25.27.24 can accommodate only two hosts. The mask 255.255.255.252 leaves 2 host bits in the mask and when we plug that into the formula we get 22 - 2, which equals 2.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco > Design Tech Notes > IP Routing > IP Addressing and Subnetting for New Users > Understanding IP Addresses > Document ID: 13788

Question 260

Which Cisco IOS command disables Cisco Discovery Protocol Version 2 (CDPv2) advertisements?

- ☒ no cdp advertise-v2
- ☐ no cdp v2-advertise
- ☐ no cdp run
- ☐ no cdp enable

Explanation:

Explanation:

The no cdp advertise-v2 command disables CDPv2 advertisements. It is the reverse of the cdp advertise-v2 command, which enables CDPv2 advertisements on a device.

The no cdp v2-advertise command is not a valid Cisco IOS command.

The no cdp run command disables CDP, not CDPv2 advertisements.

The no cdp enable command disables CDP on an interface.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Support > Using Cisco Discovery Protocol

Question 261

You have implemented SNMP v3 in your network. After making the configuration changes, you find that technicians in the TECHS group cannot access the MIB. You execute the show run command and receive the following output that relates to SNMP:

```
<output omitted>

snmp-server group NORMAL v3 priv read NORMAL write NORMAL
snmp-server group TECHS v3 priv read TECHS access 99
snmp-server group TRAP v3 priv

!!
snmp-server user NORMAL NORMAL v3 auth sha CISCO priv des56 CISCO
snmp-server user TECHS TECHS v3 auth sha CISCO priv des56 CISCO
snmp-server user TRAP TRAP v3 auth sha CISCO priv des56 CISCO

snmp-server enable traps snmp linkup linkdown
snmp-server host 155.1.146.100 traps version 3 priv TRAP
```

What is preventing the TECHS group from viewing the MIB?

- ☐ The presence of the keyword priv in the command creating the RESTRICTED group
- ☐ A mismatch between the authentication mechanism and the encryption type in the command creating the TECHS user
- ☒ The absence of an access list defining the stations that can used by the TECHS group
- ☐ The presence of the keyword auth in the command creating the TECHS user

Explanation:

Explanation:

The command that creates the TECHS group ends with the parameter access 99:

snmp-server group TECHS v3 priv read TECHS access 99

This indicates that the access list number 99 is specifying the IP addresses of the stations allowed to connect to the MIB for the group. Since the access list is missing from the configuration, no IP addresses will be allowed, and no connections can be made by the group.

The presence of the keyword priv in the command creating the TECHS group is not causing the issue. This keyword indicates that encryption (privacy) and authentication should both be used on all transmissions by the group.

 Licensed to Berend Post berend.post@it-university.nl

In SMNPv3, there are three combinations of security that can be used:

noAuthNoPriv- no authentication and no encryption; includes the noauth keyword in the configuration

AuthNoPriv - messages are authenticated but not encrypted; includes the auth keyword in the configuration

AuthPriv - messages are authenticated and encrypted; includes the priv keyword in the configuration

There is no mismatch between the authentication mechanism and the encryption type in the command creating the TECHS user.

snmp-server user TECHS TECHS v3 auth sha CISCO priv des56 CISCO

In the preceding command, the section auth sha CISCO specified that messages are authenticated using SHA with a key of CISCO. It does not need to the match the section priv des56 CISCO, which indicates that encryption (priv) will be provided using DES56 with a key of CISCO.

The presence of the keyword auth in the command creating the TECHS user is not causing the issue. This line indicates that that messages are authenticated using SHA with a key of CISCO.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device-monitoring protocols

References:

SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) > SNMPv3

Question 262

Which of the following is a classful routing protocol?

- ☒ RIPv1
- ☐ EIGRP
- ☐ BGPv4
- ☐ RIPv2

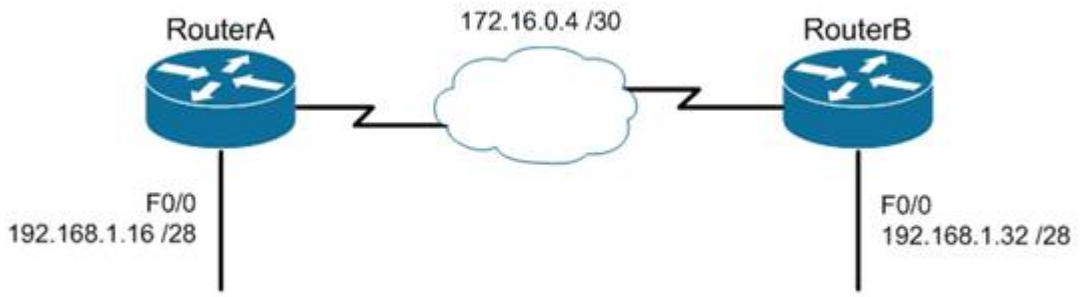
Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The Routing Information Protocol version 1 (RIPv1) is a classful routing protocol, which exchanges routes without including any subnet masking information. IP addresses in the routing table should have the same subnet mask. Because classful routing protocols may not fully utilize the available IP address range, all router interfaces within the same network must have the same subnet mask.

Open Shortest Path First (OSPF), Routing Information Protocol version 2 (RIPv2), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol version 4 (BGPv4) are classless routing protocols. These protocols include the subnet mask in the route advertisement and support variable length subnet masks (VLSM). Intermediate System-to-Intermediate System (IS-IS) is also a classless routing protocol. An example of a network using VLSM is shown below. Note the different masks used, indicated with CIDR notation.



Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

Cisco > Articles > Cisco Networking Academy > CCNP 1: Advanced IP Addressing Management

Cisco > Internetworking Technology Handbook > Routing Information Protocol (RIP)

Licensed to Berend Post berend.post@it-university.nl

Question 263

The following is a partial output of the show interfaces command:

```
Serial 0 is up, line protocol is down
Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
Internet address is 134.108.28.8, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 4 packets/sec
1127576 packets input, 447251251 bytes, 0 no buffer
Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
5332142 packets output, 496316039 bytes, 0 underruns
0 output errors, 432 collisions, 0 interface resets, 0 restarts
<<output omitted>>
```

What does the Serial 0 is up, line protocol is down statement signify in the output? (Choose all that apply.)

- ☐ the shutdown interface command is present in the router configuration
- ☐ a cable is unplugged
- ☐ the interface is displaying normal operation
- ☒ there are no problems with physical connectivity
- ☒ there is a configuration problem in the local or remote router

Explanation:

Explanation:

The Serial 0 is up, line protocol is down statement in the output signifies the following:

There are no problems with the physical connectivity.

There is a configuration problem in the local or remote router.

The remote router might not be sending the keep-alives.

There may be a problem with the leased lines such as line noise and a malfunctioning switch.

There is an incorrect configuration of the CSU/DSU, which can cause timing issues on the cable.

The local or remote CSU/DSU might have failed.

The option stating that the shutdown interface command is present in the router configuration is incorrect because if the shutdown interface command is present in the router configuration, the message displayed would be Serial 0 is administratively down, line protocol is down.

 Licensed to Berend Post berend.post@it-university.nl

The option stating that a cable is unplugged is incorrect because that would be indicated by Serial 0 is down, line protocol is down. Physical problems such as a bad cable or cable unplugged are addressed in the first part of the output (serial0 is up/down).

The option stating that the message refers to normal operation of the interface is incorrect because the line protocol is shown as down, which indicates a problem.

Objective:

Routing Fundamentals

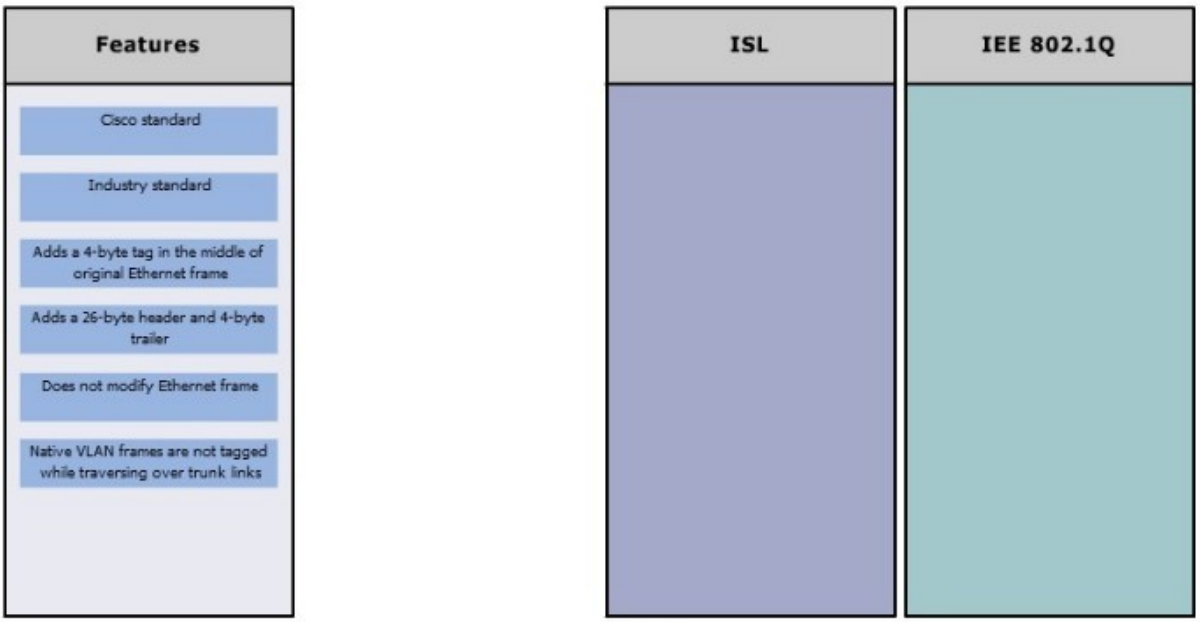
Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

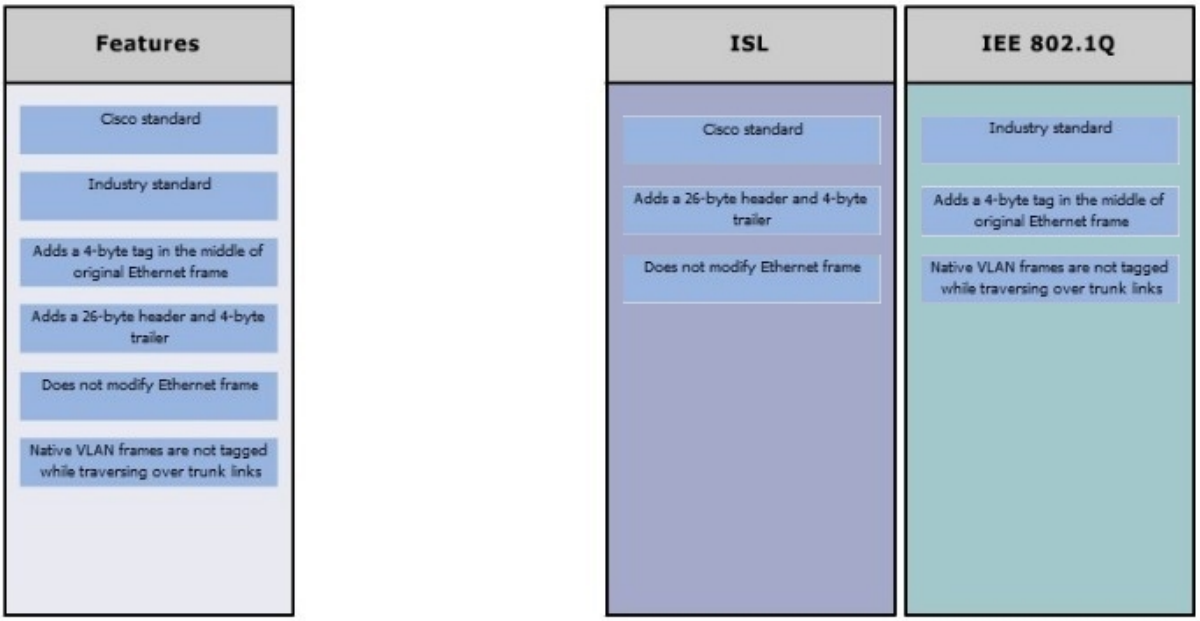
Question 264

DRAG DROP
Click and drag the features on the left to their corresponding frame tagging method on the right.



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

Explanation:

ISL and IEEE 802.1Q are VLAN frame tagging methods.

ISL:

Is Cisco proprietary

Adds a 26-byte header and 4-byte trailer

Does not modify Ethernet frame

IEEE 802.1Q frame tagging method:

Is a standard method

Adds a 4-byte tag in the middle of original Ethernet frame

Has a concept called native VLAN. Native VLAN frames are not tagged while traversing over a trunk link.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot interswitch connectivity

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format > Document ID: 17056

Question 265

Examine the network diagram.



Which switch port(s) will be in a forwarding state? (Choose two.)

- ☒ SwitchA - Fa0/1 and Fa0/2
- ☐ SwitchA - Fa0/1
- ☐ SwitchA - Fa0/2
- ☒ SwitchB - Fa0/1
- ☐ SwitchB - Fa0/2

Explanation:

Explanation:

Both switch ports on Switch A and Fa0/1 on Switch B will be in a forwarding state. Switch A will become the STP root bridge due to its lower MAC address. All ports on the root bridge will become designated ports in a forwarding state. Switch B has redundant connectivity to the root bridge, and must block one of its interfaces to prevent a switching loop. Both interfaces are the same speed (FastEthernet), and thus their cost to the root is the same. Finally, the interface with the lowest number will become the forwarding port. F0/1 has a lower port number than F0/2, so F0/1 becomes a forwarding port, and F0/2 becomes a blocking port.

In this scenario there are only two switches in the diagram. However, if there were more switches and Switch A were not the root bridge, the result would be the same with regard to the ports between Swicth A and B. Whenever there are redundant links between switches, one of the four ports involved will be set to a blocking (or in the case of RSTP, discarding) mode. The logic will still be the same, since the cost to get to the root bridge will still be equal if the port speeds are equal.

Licensed to Berend Post berend.post@it-university.nl

Without STP (which can be disabled) operating on switches with redundant links, such as those in the figure, loops can and almost surely will occur. For example, if a host connected to SwitchA were to send an ARP request for the MAC address of a host connected to SwitchB, the request could loop and cause a broadcast storm, slowing performance dramatically. This would probably occur when any host connected to either switch sends a broadcast frame, such as a DHCP request.

Rapid Spanning Tree Protocol (RSTP) uses the term discarding for a switch port that is not forwarding frames.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and TechNotes > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

Licensed to Berend Post berend.post@it-university.nl

Question 266

Which command produced the following output?

```
<output omitted>
Routing Process "ospf 203" with ID 21.0.0.1 and Domain ID 21.20.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 10 secs, Hold time between two SPFs 20 secs
Minimum LSA interval 10 secs. Minimum LSA arrival 5 secs
LSA group pacing timer 200secs
Interface flood pacing timer 110 msecs
Retransmission pacing timer 110 msecs
Number of external LSA 1. Checksum Sum 0x0
Number of opaque AS LSA 1. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 3. 1 normal 0 stub 1 nssa
External flood list length 0

Area BACKBONE(0)
Number of interfaces in this area is 4
Area has message digest authentication
SPF algorithm executed 6 times
Area ranges are
Number of LSA 3. Checksum Sum 0x29BEB
Number of opaque link LSA 1. Checksum Sum 0x0
Number of DCbitless LSA 3
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

- ☐ show ip ospf database
- ☐ show ip ospf statistics
- ☒ show ip ospf
- ☐ show ip ospf traffic

Explanation:

Explanation:

The output was produced by the show ip ospf command. The show ip ospf command is used to view information about the OSPF routing processes. The syntax of the command is as follows:

Router# show ip ospf [process-id]

The process-id parameter of the command specifies the process ID.

The show ip ospf database command is incorrect because this command is used to view the OSPF database for a specific router. The following is sample output from the show ip ospf database command when no arguments or keywords are used:

 Licensed to Berend Post berend.post@it-university.nl

```
Router# show ip ospf database
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Router Link States(Area 0.0.0.0)
Link ID ADV Router Age Seq# Checksum Link count
172.16.21.6 172.16.21.6 1724 0x80002CFB 0x69BC 5
172.16.21.5 172.16.21.5 2512 0x800009D2 0xA2B8 3
172.16.1.2 172.16.1.2 1659 0x80000A98 0x4CB6 7
172.16.1.1 172.16.1.1 5115 0x800009B6 0x5F2C 9
172.16.1.5 172.16.1.5 1626 0x80002BC 0x2A1A 4
172.16.65.6 172.16.65.6 1315 0x80001947 0xEEE1 9
172.16.241.5 172.16.241.5 1123 0x8000007C 0x7C70 1
172.16.27.6 172.16.27.6 1712 0x80000548 0x8641 4
172.16.70.6 172.16.70.6 1142 0x80000B97 0xEB84 6
Displaying Net Link States(Area 0.0.0.0)
Link ID ADV Router Age Seq# Checksum
172.16.1.3 192.168.239.66 1245 0x800000EC 0x82E
Displaying Summary Net Link States(Area 0.0.0.0)
Link ID ADV Router Age Seq# Checksum
172.16.240.0 172.16.241.5 1152 0x80000077 0x7A05
172.16.241.0 172.16.241.5 1152 0x80000070 0xAEB7
172.16.244.0 172.16.241.5 1152 0x80000071 0x95CB
```

The show ip ospf statistics command is incorrect because this command is used to view the OSPF calculation statistics. The following is sample output from the show ip ospf statistics command that shows a single line of information for each SPF calculation:

```
Router# show ip ospf statistics
OSPF process ID 200
----------------------------------------
Area 0: SPF algorithm executed 10 times
Area 200: SPF algorithm executed 8 times
Summary OSPF SPF statistic
SPF calculation time
Delta T Intra D-Intra Summ D-Summ Ext D-Ext Total Reason
08:17:16 0 0 0 0 0 0 0 R,
08:16:47 0 0 0 0 0 0 0 R, N,
08:16:37 0 0 0 0 0 0 0 R, X
00:04:40 208 40 208 44 220 0 720 R, N, SN, X
00:03:15 0 112 4 108 8 96 328 R, N, SN, X
00:02:55 164 40 176 44 188 0 612 R, N, SN, X
00:01:49 0 4 4 0 4 4 16 R, N, SN, X
00:01:48 0 0 4 0 4 0 12 R, N, SN, SA, X
00:01:43 0 0 4 0 4 0 8 R,
00:00:53 164 40 176 44 188 0 612 R, N, SN, X
```

The show ip ospf traffic command is incorrect because this is not a valid command.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast interior and exterior routing protocols

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Cisco IOS IP Routing Protocols Command Reference > OSPF Commands: show ip ospf through T > show ip ospf

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 9: OSPF, p. 375.

Question 267

What is the primary benefit of the Virtual Local Area Network (VLAN) Trunking Protocol (VTP)?

- ☐ broadcast control
- ☐ frame tagging
- ☐ inter-VLAN routing
- ☒ consistent VLAN configuration across switches in a domain

Explanation:

Explanation:

VTP manages configured VLANs across a switched network and maintains consistency of VLAN information throughout a VTP domain. When an administrator adds, deletes, or renames VLANs, VTP propagates this information to all other switches in the VTP domain. This makes the process of VLAN changes a plug-and-play activity. This protocol was developed by, and remains proprietary to Cisco Systems.

Broadcast control is not the primary benefit of VTP. Broadcast control is achieved by using VLANs. VLANs segment the network into logical broadcast domains. This helps in the reduction of unnecessary traffic over the network and optimizes the available bandwidth use. VTP pruning helps reduce broadcast and unknown unicast over VLAN trunk links. However, this is not the primary benefit of VTP.

Frame tagging is required for VLAN identification as frames traverse trunk links in a switch fabric. Inter-Switch Link (ISL) and IEEE 802.1q are the two methods of frame tagging available on Cisco devices. ISL is proprietary to Cisco, whereas IEEE 802.1q is a standard method. VTP is not a frame tagging method.

Inter-VLAN routing is achieved by an Open Systems Interconnect (OSI) Layer 3 device (Router). Inter-VLAN routing is not a benefit of VTP.

Objective:

LAN Switching Fundamentals

Sub-Objective:

 Licensed to Berend Post berend.post@it-university.nl

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Cisco > Support > LAN Switching > Virtual LANS / VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Configuring VLAN Trunk Protocol (VTP) > Document ID: 98154

Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25) > Understanding and Configuring VLANs, VTP, and VMPS

Question 268

Which of the following is NOT true of APIC-EM?

- ☒ It supports greenfield but not brownfield deployments
- ☐ It provides a single point for network automation
- ☐ It saves time and cost
- ☐ It is open and programmable

Explanation:

Explanation:

Cisco Application Policy Infrastructure Controller Enterprise Module (APIC_EM) is an SDN controller platform that supports both greenfield implementations, which use no previous code and design from the ground up, and brownfield implementations, which incorporate existing code.

APIC-EM does provide a single point for network automation. This automation leads to both time and cost savings.

APIC-EM uses an open and programmable approach to devices, policies, and analytics.

Objective:

Infrastructure Security

Sub-Objective:

Verify ACLs using the APIC-EM Path Trace ACL analysis tool

References:

Products & Services > Cloud and Systems Management > Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) > Data Sheets and Literature > Data Sheets > Cisco Application Policy Infrastructure Controller - Enterprise Module Data Sheet

Licensed to Berend Post berend.post@it-university.nl

Question 269

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?

- ☐ show cdp
- ☐ show cdp entry
- ☐ show cdp neighbor entries
- ☒ show cdp neighbors detail

Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl

```
Device ID: RTR2511
Entry address(es):
IP address: 178.10.20.1
Platform: cisco 2511, Capabilities: Router
Interface Serial 0
Holdtime : 123 sec
<output omitted>

----------------------------------------
Device ID: RTR2611-Edge
Entry address(es):
IP address: 10.10.1.2
Platform: cisco 2611, Capabilities: Router
Interface Ethernet 0
Holdtime : 123 sec
<output omitted>
```

The show cdp command is incorrect because this command is used to view global CDP information such as the timer and hold time.

The show cdp entry command is incorrect because this command is used to view information about a specific neighboring device.

The show cdp neighbor entries command is incorrect because this is not a valid Cisco IOS command.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Cisco IOS Network Command Reference, Release 12.4 > show cdp neighbors

Licensed to Berend Post berend.post@it-university.nl

Question 270

Refer to the following sample output:

```
*: interface is up
IHQ: pkts in input hold queue IQD: pkts dropped from input queue
OHQ: pkts in output hold queue OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec) RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec) TXPS: tx rate (pkts/sec)
TRTL: throttle count
Interface IHQ IQD OHQ OQD RXBS RXPS TXBS TXPS TRTL
------------------------------------------------------------------------
* FastEthernet0/0 0 0 0 0 0 0 0 0 0
Serial0/0 0 0 0 0 0 0 0 0 0
FastEthernet0/1 0 0 0 0 0 0 0 0 0
Serial0/1 0 0 0 0 0 0 0 0 0
```

Which Cisco Internetwork Operating System (IOS) command produces this output?

- ☐ show interfaces
- ☒ show interfaces summary
- ☐ show interfaces serial fast-ethernet
- ☐ show interfaces fast-ethernet 0/0

Explanation:

Explanation:

The show interfaces summary command will produce the given output. This command provides a summarized view of all interfaces configured on a device.

The show interfaces command is incorrect because this command does not produce the displayed output. This command is used to view information regarding statistics for specific interfaces. Without specifying an interface, a section for each interface will display, as in the example below for FastEthernet0:

Licensed to Berend Post berend.post@it-university.nl

```
FastEthernet0 is up, line protocol is down
Hardware is Fast Ethernet, address is 0019.e818.a3dd (bia
0019.e818.a3dd)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
--More
```

The show interfaces serial fast-ethernet command is incorrect because this is not a valid Cisco IOS command.

The show interfaces fast-ethernet 0/0 command is incorrect. Although it produces similar output, that output only relates to the FastEthernet 0/0 interface. An example of this output follows:

Licensed to Berend Post berend.post@it-university.nl

```
FastEthernet0 is up, line protocol is up
Hardware is Fast Ethernet, address is 0019.e818.a3dd (bia
0019.e818.a3dd)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops:105
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 1530000 bits/sec, 201 packets/sec
5 minute output rate 673000 bits/sec, 173 packets/sec
404737363 packets input, 23875417953 bytes, 11 no buffer
Received 1206930011 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
401877661 packets output, 23875417953 bytes, 0 underruns
0 output errors, 576297 collisions, 0 interface resets
0 babbles, 0 late collision, 2174225 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Notice that the line of output that says FastEthernet0 is up, line protocol is up indicates that Layers 1 to 3 of the OSI Model are functioning correctly. Also, in the lower portion, there are no values in the error counters such as input errors, output errors, and so on. Finally, make note in line 8 where the interface is set to autosense both the duplex and the speed. Duplex and speed must be in agreement between the NIC on the host and the switch port.

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

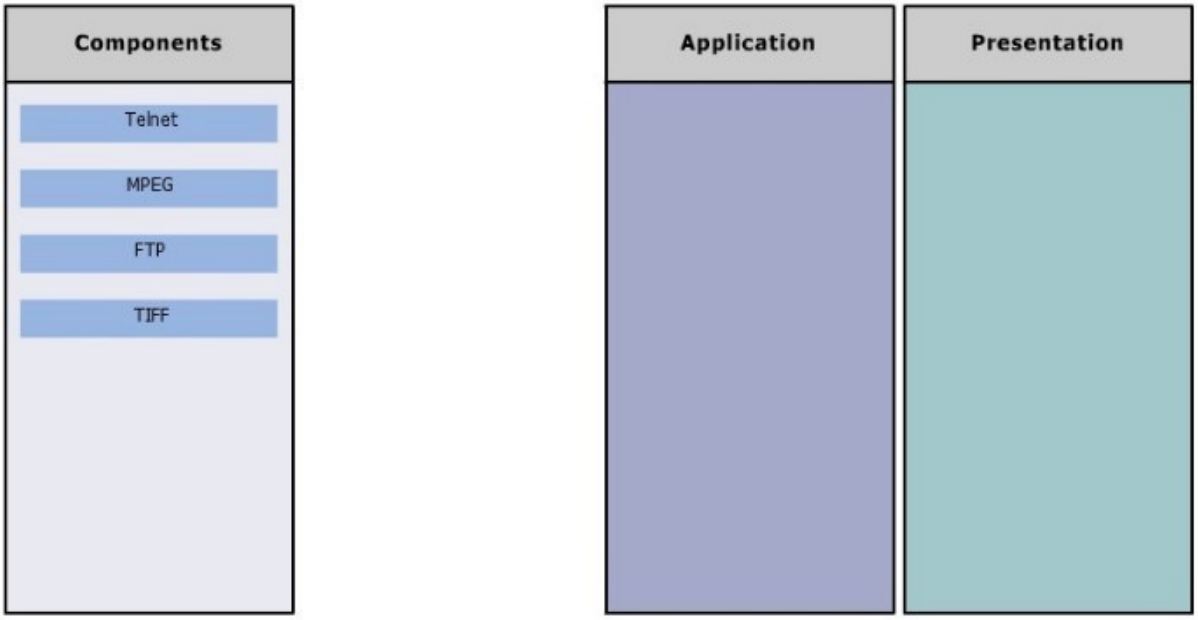
References:

Cisco > Cisco IOS Interface and Hardware Component Command Reference > show interfaces summary

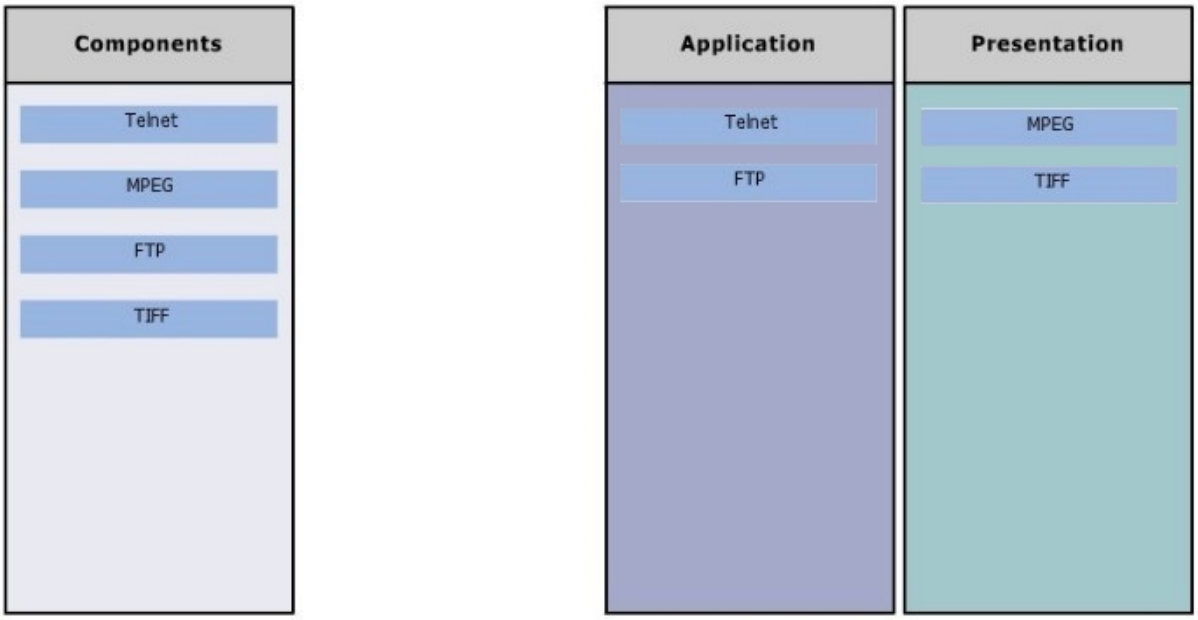
Licensed to Berend Post berend.post@it-university.nl

Question 271

DRAG DROP
Click and drag the components on the left to their corresponding layers of the Open Systems Interconnection (OSI) model on the right.



Solution:



Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

Motion Picture Experts Group (MPEG) and Tagged Image 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 protocols which 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:

Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems

Question 272

Which of the following commands will configure a router to use DNS for hostname resolution?

- ☐ ip dns primary
- ☒ ip domain lookup
- ☐ ip dns server
- ☐ ip name-server

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The ip domain lookup command configures the device to use DNS for hostname resolution. It must be accompanied by a command that specifies the location of the DNS server, which is done with the ip name-server command.

The ip dns-primary command is used to configure the device as the primary DNS name server for a domain (zone) and as the start of authority (SOA) record source, which designates the start of a zone.

The ip dns server command is used to make the device a DNS server.

Objective:

Infrastructure Services

Sub-Objective:

Describe DNS lookup operation

References:

Home > Support > IP Addressing: DNS Configuration Guide, Cisco IOS Release 15M&T

Question 273

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?

- ☒ router(config)#ip nat inside source static 192.168.144.25 202.56.63.102
- ☐ router(config)#ip source nat inside static local-ip 192.168.144.25 global-ip 202.56.63.102
- ☐ router(config)#ip nat static inside source 192.168.144.25 202.56.63.102
- ☐ router(config)#ip nat inside static source 192.168.144.25 202.56.63.102

Explanation:

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

 Licensed to Berend Post berend.post@it-university.nl

This static configuration can be removed by entering the global no ip nat inside source static command.

Simply executing the ip nat inside source command will not result in NAT functioning. The NAT process also has to be applied correctly to the inside and outside interfaces. For example if, in this scenario the Fa0/0 interface hosted the LAN and the S0/0 interface connected to the Internet the following commands would complete the configuration of static NAT.

Router(config)#interface F0/0

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#interface S0/0

Router(config-if)#ip nat outside

The other options are incorrect because they are not valid Cisco IOS configuration commands. They all contain syntax errors.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot inside source NAT

References:

Question 274

Which command would you use to see which interfaces are currently operating as trunks?

- ☐ show interface switchports
- ☐ show trunk interface
- ☒ show interfaces trunk
- ☐ show switchport trunk

Explanation:

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:

 Licensed to Berend Post berend.post@it-university.nl

Switch# show interfaces trunk

Port Mode Encapsulation Status Native vlan

Gi0/1 desirable 802.1q trunking 1

Gi0/2 desirable 802.1q trunking 1

Port Vlans allowed on trunk

Gi0/1 1-4094

Gi0/2 1-4094

<<output omitted>>

This output indicates that switch ports Gi0/1 and Gi0/2 are both currently operating as trunks (Status), and that 802.1q frame tagging is being used on the trunk links.

The remaining options are incorrect because they are not valid Cisco IOS commands.

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Licensed to Berend Post berend.post@it-university.nl

Question 275

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.)

- ☐ the interface is functional
- ☒ the largest frame allowed through this connection is 1500 bytes
- ☒ the interface needs the no shutdown command executed to be functional
- ☐ the largest frame allowed through this connection is 10000 Kbs

Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Question 276

Which Cisco Internetwork Operating System (IOS) command is used to assign a router a name for identification?

- ☐ description
- ☐ banner motd
- ☒ hostname
- ☐ banner exec

Explanation:

Explanation:

The hostname command is used to assign the router a name for identification. This command is a global configuration mode command. The syntax of the command is as follows:

Router(config)# hostname [name]

The name parameter of the command specifies the new host name for the router.

The description command is incorrect because this command is used to set a description for an interface. The description command is an interface configuration mode command.

The banner motd command is used to specify a message of the day (MOTD) banner to users logging into the router. This is a global configuration mode command, but it does not assign a name to the router for identification.

The banner exec command enables a banner message to be displayed when an EXEC process is created; for example, if a line is activated or an incoming connection is made to a telnet line.

Objective:

Network Fundamentals

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

Cisco > Cisco IOS Configuration Fundamentals Command Reference > F through K > hostname

Licensed to Berend Post berend.post@it-university.nl

Question 277

What command produced the following output?

```
Routing Protocol is "igrp 120"
Sending updates every 90 seconds, next due in 44 seconds
Invalid after 270 seconds, hold down 280, flushed after 630
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
IGRP maximum hopcount 100
IGRP maximum metric variance 1
Redistributing: igrp 109
Routing for Networks:
172.160.74.0
Routing Information Sources:
Gateway Distance Last Update
172.160.74.18 100 0:56:41
172.160.74.19 100 6d19
172.160.74.22 100 0:25:41
172.160.74.20 100 0:01:04
172.160.74.30 100 0:02:29
Distance: (default is 100)
Routing Protocol is "bgp 18"
Sending updates every 60 seconds, next due in 0 seconds
Outgoing update filter list for all interfaces is 1
Incoming update filter list for all interfaces is not set
Redistributing: igrp 109
IGP synchronization is disabled
Automatic route summarization is enabled
Neighbor(s):
Address FiltIn FiltOut DistIn DistOut Weight RouteMap
192.109.211.17 1
192.109.213.89 1
198.6.255.13 1
172.161.72.18 1
172.161.72.19
172.161.84.17 1
Routing for Networks:
192.108.209.0
192.108.211.0
198.6.254.0
Routing Information Sources:
Gateway Distance Last Update
172.161.72.19 20 0:05:28
Distance: external 20 internal 200 local 200
```

- ☐ show ip process
- ☐ show ip route
- ☒ show ip protocols
- ☐ show ip routing process

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The show ip protocols command is used to view the current state of active routing protocols. This command is issued from Privileged EXEC mode. It has the following syntax:

Router# show ip protocols

This command does not have any parameters.

The output was not produced by the command show ip process or the show ip routing process. The show ip routing process and show ip process commands are incorrect because these are not valid Cisco IOS commands.

The output was not produced by the command show ip route. The show ip route command is is used to view the current state of the routing table. An example of the output is shown below.

```
router>show ip route
Codes: C - connected O - OSPF i - IS-IS
S - static IA - inter area L1 - level-1
B - BGP E1 - external type 1 L2 - level-2
E2 - external type 2
* - candidate default
m - route's metric
w - route's weight
S 0.0.0.0/0 directly connected to null 0
C 6.1.1.64/28 directly connected to ethernet 1
C 6.1.1.80/28 directly connected to ethernet 2
C 6.1.1.96/28 directly connected to ethernet 3
C 6.1.1.112/28 directly connected to ethernet 4
S 11.1.0.0/16 via 10.5.0.1 [w:0 m:0]
C 11.5.0.0/16 directly connected to ethernet 0
S 127.0.0.0/8 directly connected to null 0
```


Licensed to Berend Post berend.post@it-university.nl

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 11: Troubleshooting Routing Protocols, pp. 410-413.

Question 278

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?

- ☐ ip dhcp restrict 10.1.0.254
- ☒ ip dhcp excluded-address 10.1.0.253
- ☐ ip dhcp excluded-address 10.1.0.254
- ☐ ip dhcp 10.1.0.253 excluded-address

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

You would not execute ip dhcp excluded-address 10.1.0.254. This is the address of the router and it will automatically be excluded.

The other commands are incorrect because they are not valid Cisco IOS commands.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify DHCP on a router (excluding static reservations)

References:

Cisco > Support > Cisco IOS Software > Configuring the Cisco IOS DHCP Server > Excluding IP Addresses

Question 279

Which of the following situations could cause a switch to enter initial configuration mode upon booting?

- ☐ Corrupt or missing image file in flash memory
- ☒ Corrupt or missing configuration file in NVRAM memory
- ☐ Corrupt or missing configuration file in flash memory
- ☐ Corrupt or missing configuration file in ROM memory

Explanation:

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:

 Licensed to Berend Post berend.post@it-university.nl

Infrastructure Management

Sub-Objective:

Configure and verify initial device configuration

References:

Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 6: Using the Cisco IOS Integrated File System > NVRAM File System Management

Cisco > Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 > Part 11: Rebooting > Rebooting and Reloading - Configuring Image Loading Characteristics

Question 280

Which Cisco IOS command is used on a Cisco Catalyst 6500 series switch to view the spanning-tree protocol (STP) information for a virtual LAN (VLAN)?

- ☐ show spanning tree
- ☒ show spanning-tree vlan
- ☐ show spantree
- ☐ show spantree vlan

Explanation:

Explanation:

The show spanning-tree vlan Cisco IOS command is used on a Catalyst 6500 series switch to view the spanning-tree information for a VLAN, such as information on the root switch (bridge ID, root path, root cost), as well as local switch.

The following is sample output of the show spanning-treevlan vlan-id command:

Licensed to Berend Post berend.post@it-university.nl

```
Switch# show spanning-tree vlan 1
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 000c.00d3.5124
Cost 19
Port 2 (FastEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000c.14f5.b5c0
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

The show spanning tree command is incorrect because it is not the correct syntax of a Cisco IOS command.

The show spantree and show spantree vlan commands are incorrect because these are CatOS commands, not Cisco IOS commands.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Cisco IOS LAN Switching Command Reference > show spanning-tree

Licensed to Berend Post berend.post@it-university.nl

Question 281

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?

- ☐ There is no problem with the physical connectivity.
- ☐ There is a configuration problem in the local or remote router.
- ☐ There is a problem at the telephone company's end.
- ☒ The shutdown interface command is present in the router configuration.

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

This line does not show that there is a problem at the telephone company's end. Since the interface is administratively shut down, there is no way of determining the operational status of the physical layer or protocol layer on the other end of the line.

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Question 282

With which type of service is bandwidth and latency the biggest consideration?

- ☒ streaming video
- ☐ telnet sessions
- ☐ FTP transfers
- ☐ authentication traffic

Explanation:

Explanation:

Streaming video places the largest demand on both bandwidth and latency. Video traffic is real-time and benefits from dedicated bandwidth with QoS implementation to ensure quality. Moreover, this service can tolerate very little latency.

Telnet and FTP sessions are both low bandwidth users and can tolerate a high degree of latency since the data can be reassembled when all pieces arrive, which is not possible when data is coming in real-time, and waiting for retransmissions and reassembly is not feasible.

Authentication traffic is not sensitive to latency and does not require much bandwidth either.

Objective:

WAN Technologies

Sub-Objective:

Describe basic QoS concepts

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco Documentation > Internetworking Technology Handbook > Voice/Data Integration Technologies

Question 283

Which Cisco IOS interface configuration command is used to configure the private VLAN edge ports on a Cisco Catalyst 2950 switch?

- ☒ switchport protected
- ☐ switchport port-security
- ☐ switchport port-vlan-edge
- ☐ switchport port-security violation

Explanation:

Explanation:

The switchport protected interface configuration command is used to configure protected ports (private VLAN edge ports) on a Cisco Catalyst 2950 switch. A protected port cannot directly communicate with any other protected port on the same switch. It is used in cases where an application requires that no traffic be directly passed from port to port on the same switch. All traffic through the protected port must be transmitted via a Layer 3 device, such as a router.

The switchport port-security command enables basic switch port security. With this command, you can define a group of source MAC addresses (called an address table) that are allowed to access the port. The switch will not forward any packets to the port with source addresses that do not match this group. This is one method a network administrator can use to prevent unauthorized access to the LAN by only allowing company-known MAC addresses. Controlling which MAC addresses can access a port has the following advantages:

It can ensure full bandwidth on the port if the table is limited to a single source address.

It can make the port more secure by preventing access from unknown MAC addresses. It can also be used to prevent access on unused ports to prevent unauthorized hosts from accessing the LAN.

The switchport port-security violation command further defines actions a switch can take on the interface in the event of a security violation by following the command with a choice from the {shutdown | restrict | protect} options.

The switchport port-vlan-edge command is incorrect because this is not a valid Cisco command.

Objective:

Infrastructure Security

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

Question 284

Which of the following statements describes split horizon?

- ☐ The router learns from its neighbor that a route has gone down, and the router sends an update back to the neighbor with an infinite metric to that route.
- ☐ For a period of time, the router will ignore any route advertisements with a lower metric to a downed route.
- ☒ A router will not send route information back out the same interface over which it was learned.
- ☐ The moment a router determines a route has gone down, it will immediately send a route update with an infinite metric to that route.
- ☐ The packets are flooded when a topology change occurs, causing network routers to update their topological databases and recalculate routes.

Explanation:

Explanation:

Split horizon is used to prevent routing loops in distance vector routing environments. It prevents a router from advertising a network back in the direction of the router from which it was learned. In this sense, route advertisements flow "downstream" (away from the route), but never "upstream" (back towards the advertised route).

Poison reverse describes when a router learns that a network has gone down, and the router sends an update back to the neighbor with an infinite metric.

Holddown describes when a router ignores any route advertisements that have a lower metric to a downed route.

Triggered updates describe when a router immediately sends a route update with an infinite metric, as opposed to waiting for its next regularly scheduled routing update.

Link State Advertisements (LSA) are packets that are flooded when a topology change occurs, causing network routers to update their topological databases and recalculate routes.

Objective:

 Licensed to Berend Post berend.post@it-university.nl

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

Cisco > Articles > Network Technology > General Networking > Dynamic Routing Protocols

Question 285

You have been asked to troubleshoot the NTP configuration of a router named R70. After executing the show run command, you receive the following partial output of the command that shows the configuration relevant to NTP:

clock timezone PST -8
clock summer-time PDT recurring
ntp update-calendar
ntp server 192.168.13.57
ntp server 192.168.11.58
interface Ethernet 0/0
ntp broadcast

Based on this output, which of the following statements is true?

- ☐ the time zone is set to 8 hours less than Pacific Standard time
- ☐ the router will listen for NTP broadcasts on interface E0/0
- ☒ the router will send NTP broadcasts on interface E0/0
- ☐ the router will periodically update its software clock

Explanation:

Explanation:

The router will send NTP broadcast on its E0/0 interface. The command ntp broadcast, when executed under an interface, instructs the router to send NTP broadcast packets on the interface. Any devices on the network that are set with the ntp broadcast client command on any interface will be listening for these NTP broadcasts. While the clients will not respond in any way, they will use the information in the NTP broadcast packets to synchronize their clocks with the information.

The time zone is not set to 8 hours less than Pacific Standard Time. The value -8 in the command clock timezone PST -8 represents the number of hours of offset from UTC time, not from the time zone stated in the clock timezone command.

The router will not listen for NTP broadcasts on the interface E0/0. The ntp broadcast command, when executed under an interface, instructs the router to send NTP broadcast packets on the

 Licensed to Berend Post berend.post@it-university.nl

interface. To set the interface to listen and use NTP broadcasts, you would execute the ntp broadcast client command on the interface.

The router will not periodically update its software clock. The command ntp update-calendar configures the system to update its hardware clock from the software clock at periodic intervals.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify NTP operating in a client/server mode

References:

Basic System Management > Setting Time and Calendar Services > Configuring NTP

Question 286

Which of the following methods will ensure that only one specific host can connect to port F0/1 on a switch?

- ☐ Configure port security on F0/1 to forward traffic to a destination other than that of the MAC address of the host.
- ☐ Configure the MAC address of the host as a static entry associated with port F0/1.
- ☒ Configure port security on F0/1 to accept traffic only from the MAC address of the host.
- ☐ Configure an inbound access control list on port F0/1 limiting traffic to the IP address of the host.
- ☐ Configure port security on F0/1 to accept traffic other than that of the MAC address of the host.

Explanation:

Explanation:

To limit connections to a specific host, you should 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:

 Licensed to Berend Post berend.post@it-university.nl

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.

The mac-address-table static command assigns a permanent MAC address to the port, but does not prevent any other MAC addresses from being associated with 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

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:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

Cisco > Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide > Configuring Port Security > Enabling Port Security

Licensed to Berend Post berend.post@it-university.nl

Question 287

Examine the output of the show ip route command below:

```
Gateway of last resort is not set

     20.0.0.0/24 is subnetted, 1 subnets
O E2    20.20.20.0 [110/20] via 192.168.1.2, 00:05:10, FastEthernet0/0
O IA 172.16.0.0/16 [50/21] via 192.168.4.1, 00:05:10, FastEthernet0/1
                   [50/21] via 192.168.1.2, 00:05:10, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/32 is subnetted, 1 subnets
C       10.10.10.10 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/20] via 192.168.1.2, 00:05:10, FastEthernet0/0
O    192.168.3.0/24 [110/20] via 192.168.4.1, 00:05:10, FastEthernet0/1
     30.0.0.0/32 is subnetted, 1 subnets
O       30.30.30.30 [50/21] via 192.168.4.1, 00:05:10, FastEthernet0/1
                    [50/21] via 192.168.1.2, 00:05:10, FastEthernet0/0
```

Which of the following statements is FALSE?

- ☐ The route to 30.30.30.30 uses a cost of 21
- ☒ The command ip route 192.168.2.0 255.255.255.0 172.16.14.2 200 will replace the current route to 192.168.2.0/24
- ☐ The route to 192.168.2.0/24 uses the default administrative distance
- ☐ Traffic will be load balanced across two routes to 30.30.30.30

Explanation:

Explanation:

The command ip route 10.10.10.0 255.255.255.0 172.16.14.2 200 will NOT replace the current route to 10.0.0.0/24.

When you execute the ip route command to enter a static route, the administrative distance can be altered by adding the desired distance value to the end of the command. In this scenario, the administrative distance value was set to 200. The route to the 10.10.10.0/24 network that is currently in the table was learned by OSPF and is using the default administrative distance of 110. Since 110 is lower than 200, the new static route will not be added to the routing table UNLESS the current route becomes unavailable.

The route to 30.30.30.30 does uses a cost of 21, as is indicated by the value on the right side of the forward slash within the brackets found in the route entry, [50/21].

The route to 192.168.2.0/24 uses the default administrative distance. It was learned from OSPF, which has a default distance of 110. Its administrative distance is indicated by the value on the left side of the forward slash within the brackets found in the route entry, [110/20].

Licensed to Berend Post berend.post@it-university.nl

Traffic will be load balanced across two routes to 30.30.30.30 because they have equal cost of 21. This cost is indicated by the value on the right side of the forward slash within the brackets found in the route entry, [50/21].

Objective:

Routing Fundamentals

Sub-Objective:

Describe how a routing table is populated by different routing information sources

References:

Cisco > Support > Cisco IOS IP Routing: Protocol-Independent Command Reference > ip route

Cisco Press > Articles > Cisco Network Technology > General Networking > Cisco Networking Academy's Introduction to Routing Dynamically

Question 288

Which prompt indicates the configuration mode at which Cisco IOS debug commands can be issued?

- ☐ router>
- ☒ router#
- ☐ router(config)#
- ☐ router(config-if)#

Explanation:

Explanation:

You would use privileged EXEC mode, as indicated by the router# prompt, to issue Cisco IOS show and debug commands. All debug commands are entered in privileged EXEC mode. A brief description of all the debugging commands can be displayed by entering the following command in privileged EXEC mode at the command line:

debug?

Debugging output consumes high CPU processing power and can leave the system unusable. The debug commands should be reserved to troubleshoot specific problems, preferably with the help of Cisco technical support staff.

The prompt router> indicates user exec mode, which provides limited access to the router.

Licensed to Berend Post berend.post@it-university.nl

The prompt router(config)# indicates global configuration mode, which allows configuration settings affecting the entire router. Passing through this mode is also required to access configuration mode for specific interfaces as well.

The prompt router(config-if)# indicates interface configuration mode, which allows configuration of the interface specified when entering this mode.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device management

References:

Cisco > Support > Cisco IOS Software > Using the Command-Line Interface in Cisco IOS Software

Question 289

You have a class C address range and are planning a network that has an average of 50 hosts per subnet.

How many host bits will have to be borrowed for subnetting so that the maximum number of subnets can be implemented?

- ☐ 1
- ☒ 2
- ☐ 3
- ☐ 4
- ☐ 6

Explanation:

Explanation:

A class C address has 8 bits in host space. By using 2 bits from the host space for subnetting, leaving 6 host bits, you can create subnets that can accommodate up to 62 hosts each (26 - 2 = 62). This will ensure that the requirement of 50 hosts per subnet is met and the maximum number of subnets is provided.

The formulas to calculate the number of subnets and hosts are:

Number of subnets = 2number-of-subnet-bits

 Licensed to Berend Post berend.post@it-university.nl

Number of hosts per subnet = 2number-of-host-bits - 2

If you take 1 bit for subnetting:

Number of subnets = 21 = 2

Number of hosts per subnet = 27 - 2 = 126

This results in a mask of 255.255.255.128 or /25. Since each subnet need not be bigger than 50, this solution would not maximize the number of subnets.

If you take 2 bits for subnetting:

Number of subnets = 22 = 4

Number of hosts per subnet = 26 - 2 = 62

This results in a mask of 255.255.255.192 or /26. This solution would create more subnets, but the subnets are smaller than the requirement.

If you take 3 bits for subnetting:

Number of subnets = 23 = 8

Number of hosts per subnet = 25 - 2 = 30

This results in a mask of 255.255.255.224 or /27. This would create more subnets, but the subnets are smaller than the requirement.

If you take 4 bits for subnetting:

Number of subnets = 24 = 16

Number of hosts per subnet = 24 - 2 = 14

This results in a mask of 255.255.255.240 or /28. This solution would create more subnets, but the subnets are smaller than the requirement.

If you take 6 bits for subnetting:

Number of subnets = 26 = 64

Licensed to Berend Post berend.post@it-university.nl

Number of hosts per subnet = 22 - 2 = 2

This mask, 255.255.255.252 or /30, yields only 2 IP addresses, but is quite commonly used on a point-to-point link, such as between two routers. This solution would create more subnets, but the subnets are smaller than the requirement.

You will always subtract 2 from the number of hosts (the formula of 2number-of-host-bits - 2) because the all-zeros bit address is reserved for the network address and the all-ones bit address is reserved for the broadcast address.

Prior to Cisco IOS Software Release 12.0, it was common practice to subtract 2 from the networks formula (2number-of-subnet-bits) to exclude addresses of all 1s and all 0s (called the all-ones subnet and subnet zero). Today that range is usable, except with some legacy systems. On certain networks with legacy software, you may need to use the previous formula (2n - 2) to calculate the number of subnets.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Cisco > Technology Support > IP > IP Addressing Services > Design TechNotes > Subnet Zero and the All-Ones Subnet > Document ID: 13711

Question 290

Which of the following is NOT a dynamic table maintained by a router running the EIGRP routing protocol?

- ☐ topology table
- ☒ CAM table
- ☐ routing table
- ☐ neighbor table

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

All are tables maintained by a router running the EIGRP routing protocol except a Content Addressable Memory (CAM) table. This table is only present on a switch. It is used to maintain the two MAC addresses involved in a conversation between computers so that the conversation can be routed once and then switched thereafter which is a much faster process.

EIGRP maintains three dynamic tables in RAM:

Neighbor table, which is a list of all neighboring EIGRP routers on shared subnets

Topology table, which contains all discovered network paths in the internetwork

Routing table, which contains the best path (based on lowest metric) to each destination

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > Enhanced Interior Gateway Routing Protocol > Document ID: 16406 > Feasible Distance, Reported Distance, and Feasible Successor

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 10: EIGRP, pp. 392-395.

Question 291

You are purchasing a device to upgrade your network. You need to determine the type of device required, as well as the number and type of required interfaces. The device will host three LAN subnets and a T1 Internet connection.

Which of the following device and interface combinations will support this requirement without providing any unnecessary interfaces or using subinterfaces?

- ☐ a switch with one Ethernet interface and three serial interfaces
- ☒ a router with one serial interface and three Ethernet interfaces
- ☐ a router with one serial interface and one Ethernet interface
- ☐ a switch with one modem and three serial interfaces

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

This deployment will require a router with one serial interface and three Ethernet interfaces. When LAN subnets and the Internet must be connected, you must deploy a device that can make decisions based on IP addresses. This is the function of a router. Each LAN subnet will require a separate Ethernet interface, and the T1 connection requires a serial interface, so the router must have one serial interface and three Ethernet interfaces.

A switch cannot be used to connect separate subnets and the Internet. This requires a router. Switches make forwarding decisions based on MAC addresses. In this deployment, decisions must be made on the basis of IP addresses. Moreover, switches only have Ethernet interfaces, so a switch could not handle the T1 connection.

A router with one serial and one Ethernet interface will not be sufficient. Each LAN subnet will require a separate Ethernet interface.

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

References:

Cisco > Home > Internetworking Technology Handbook > Internetworking Basics > Bridging and Switching Basics

Question 292

In which two situations would it be appropriate to issue the ipconfig command with the /release and /renew options? (Choose two.)

☒ When the result of running the ipconfig /all command indicates a 169.254.163.6 address
☒ When recent scope changes have been made on the DHCP server
☐ When no IP helper address has been configured on the router between the client and the DHCP server
☐ 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

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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:

Licensed to Berend Post berend.post@it-university.nl

Question 293

Which of the following statements is NOT true regarding flow control?

- ☐ It determines the rate at which the data is transmitted between the sender and receiver.
- ☐ It can help avoid network congestion.
- ☐ It manages the data transmission between devices.
- ☒ It uses a cyclic redundancy check (CRC) to identify and remove corrupted data.

Explanation:

Explanation:

It is NOT true that flow control uses a cyclic redundancy check (CRC) to identify and remove corrupted data. CRC is an error-checking schema that checks and removes corrupted data. It is a calculation that is performed at the source. Flow control uses CRC to identify corrupted data for the purpose of requesting re-transmission, but it does not use CRC to remove the corrupted data from the packet. If corruption is detected, the entire packet will be dropped.

Flow control is a function that ensures that a sending device does not overwhelm a receiving device. The following statements are TRUE regarding flow control:

Flow control controls the amount of data that the sender can send to the receiver.

Flow control determines the rate at which the data is transmitted between the sender and receiver.

Flow control of certain types can aid in routing data around network congestion

Types of flow control include windowing, buffering, and congestion avoidance:

Windowing- a process whereby the sender and receiver agree to increase or decrease the number of packets received before an acknowledgment is required based on network conditions. This packet number is called a window. When conditions are favorable, the window size will be increased. During unfavorable network conditions, it will be decreased.

Buffering- the ability of a network card to store data received but not yet processed in a buffer (memory). This enhances its ability to handle spikes in traffic without dropping any data.

Congestion avoidance - a process that some routing protocols can perform by adding information in each frame that indicates the existence of congestion on the network, allowing the router to choose a different routing path based on this information.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast OSI and TCP/IP models

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Internet Protocols > TCP Packet Format

Question 294

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?

- ☐ Ethernet 0/0 is up, line protocol is up
- ☒ Ethernet 0/0 is up, line protocol is down
- ☐ Ethernet 0/0 is down, line protocol is up
- ☐ Ethernet 0/0 is down, line protocol is down

Explanation:

Explanation:

The first or left-hand column (Ethernet 0/0 is up) indicates the Physical layer state of the interface, while the second or right-hand column (line protocol is down) indicates the Data Link layer state of the interface. The following command output excerpt indicates that the link is not functional due to a Data Link layer (or "line protocol") issue, while the Physical layer is operational:

Ethernet 0/0 is up, line protocol is down

If the problem were at the Data Link layer while the Physical layer is operational, the show interfaces command output will indicate that the interface is up, but the line protocol is down.

In the normal operation mode, when both Physical layer and Data Link layer are up, the show interfaces output will display the following message:

Ethernet0/0 is up, line protocol is up

The message Ethernet 0/0 is down, line protocol is up is not a valid output.

The message Ethernet 0/0 is down, line protocol is down indicates that both the Physical layer and the Data Link layer are down. Therefore, this is an incorrect option.

Objective:

LAN Switching Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Question 295

Your network consists of one HSRP group of six routers. All of the routers are functioning properly. The network has been stable for several days.

In which HSRP state are most of the routers?

- ☐ Learn
- ☒ Listen
- ☐ Standby
- ☐ Active

Explanation:

Explanation:

If all of the routers in the Hot Standby Routing Protocol (HSRP) group are functioning properly, then most of the routers in the group are in the listen state. Four routers will be in the listen state, one router will be in the standby state, and one router will be in the active state.

HSRP is used by a group of routers to create the appearance of a virtual router with which end stations can communicate in the event that the default gateway becomes unavailable. The active router is responsible for forwarding packets that are sent to the virtual router. The standby router is responsible for assuming the role of active router should the active router fail or become unavailable. All other HSRP routers monitor the hello messages sent by the active and standby routers. Should the active and standby routers both become unavailable, the HSRP router with the highest priority is elected to become the active router by default. For routers with equal priority values, the router with the highest IP address becomes the active router.

HSRP routers can exist in one of the following six states:

Initial

Learn

Listen

Speak

Standby

Active

Licensed to Berend Post berend.post@it-university.nl

All HSRP routers start in the initial state. A router in the learn state is waiting for its first hello message from the active router so that it can learn the virtual router's IP address. When the hello message is received and the virtual router's IP address is discovered, the HSRP router is in the listen state. A router in the listen state listens for hello messages from the active and standby routers. If an election for a new active router and a new standby router is required, then an HSRP router will enter the speak state and begin transmitting hello messages. The standby state is reserved for the standby router, and the active state is reserved for the active router. Only routers in speak, standby, and active states will transmit hello packets.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco > Home > Technology Support > IP > IP Application Services > Design > Design Technotes > Hot Standby Router Protocol Features and Functionality

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

Question 296

You have been assigned a network ID of 172.16.0.0/26. If you utilize the first network resulting from this ID, what would be the last legitimate host address in this subnet?

- ☐ 172.16.0.64
- ☐ 172.16.0.63
- ☒ 172.16.0.62
- ☐ 172.16.0.65

Explanation:

Explanation:

When a class B address such as 172.16.0.0 is subnetted with a /26 mask, the subnet mask in dotted decimal format is 255.255.255.192. This means that the interval between the network IDs of the resulting subnets is 64. The resulting network IDs are as follows:

172.16.0.0

172.16.0.64

172.16.0.128

Licensed to Berend Post berend.post@it-university.nl

172.16.0.192

172.16.1.0

and so on.

For the network ID 172.16.0.0, the last address in the range is 172.16.0.63, which is the broadcast address. Neither the network ID nor the broadcast address for any subnet can be assigned to computers. This means that the addresses that can actually be assigned range from 172.16.0.1 to 172.16.0.62. The last legitimate host address, therefore, is 172.16.0.62.

172.16.0.63 cannot be used because it is the broadcast address for the 172.16.0.0 network.

172.16.0.64 is the network ID for the 172.16.0.64 network, and 172.16.0.65 is the first address in the second network.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco > Support > IP Routing > Design TechNotes > Document ID: 13788 > IP Addressing and Subnetting for New Users

Question 297

Which subnet is IP address 172.16.5.2 /23 a member of, and what is the broadcast address for that subnet?

- ☒ subnet: 172.16.4.0, broadcast: 172.16.5.255
- ☐ subnet: 172.16.5.0, broadcast: 172.16.5.255
- ☐ subnet: 172.16.2.0, broadcast: 172.16.5.255
- ☐ subnet: 172.16.0.0, broadcast: 172.16.7.255

Explanation:

Explanation:

The IP address 172.16.5.2 /23 is a member of subnet 172.16.4.0 and has the broadcast address of 172.16.5.255. The valid host range is between 172.16.4.1 and 172.16.5.254.

 Licensed to Berend Post berend.post@it-university.nl

Binary form of IP address 172.16.5.2 = 10101100.00010000.00000101.00000010

Binary conversion for /23 netmask = 11111111.11111111.11111110.00000000

Decimal conversion for /23 netmask = 255.255.254.0

Calculations:

Perform the AND operation between the IP address and the netmask to obtain the subnet ID:

Address = 10101100.00010000.00000101.00000010

Netmask = 11111111.11111111.11111110.00000000

Subnetwork ID = 10101100.00010000.00000100.00000000

Convert the binary version of the network ID to dotted decimal format, 172.16.4.0.

To obtain the broadcast address, replace the last 9 host bits (32 - 23 = 9 bits) of the network address, which yields the following:

Binary form of broadcast address = 10101100.00011001.00000101.11111111

Decimal form of broadcast address = 172.16.5.255

Subnet	0.0	2.0	4.0
First Host	0.1	2.1	4.1
Last Host	1.254	3.254	5.254
Broadcast Address	1.255	3.255	5.255

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP AddressesCisco > Technology Support > IP > IP Addressing Services > Design TechNotes > Subnet Zero and the All-Ones Subnet > Document ID: 13711

Question 298

Which of the following NAT terms refers to a registered address that represents an inside host to an outside network?

- ☒ inside global
- ☐ outside global
- ☐ inside local
- ☐ outside local

Explanation:

Explanation:

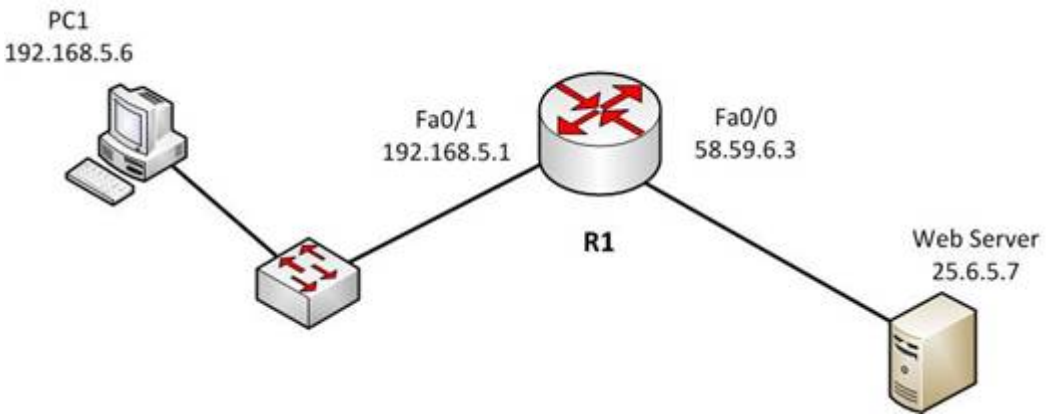
An inside global address is the registered or public address assigned by the NAT server to an inside host. To the outside world it is only address seen for the host. The real (private) address, called the inside local, remains hidden.

The outside global address is the public address of a host that is outside the network connecting to the network. It the NAT server is also translating incoming addresses as well as outgoing addresses the address it assigns to the external host is called the outside local address.

The inside local address is the private IP address assigned to a host inside the network. The outside local is the address of a host outside the network as seen by hosts inside the network.

For example, in the diagram below, PC1 is sending a packet to the Web server. R1 is operating in NAT overload mode, which means that it maps all internal private IP addresses to a single public IP address.

Licensed to Berend Post berend.post@it-university.nl



Below is a listing of the names assigned to certain addresses in the diagram:

Inside local 192.168.5.6

Inside global 58.59.6.3

Outside local 192.168.5.1

Outside global 25.67.5.7

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot inside source NAT

References:

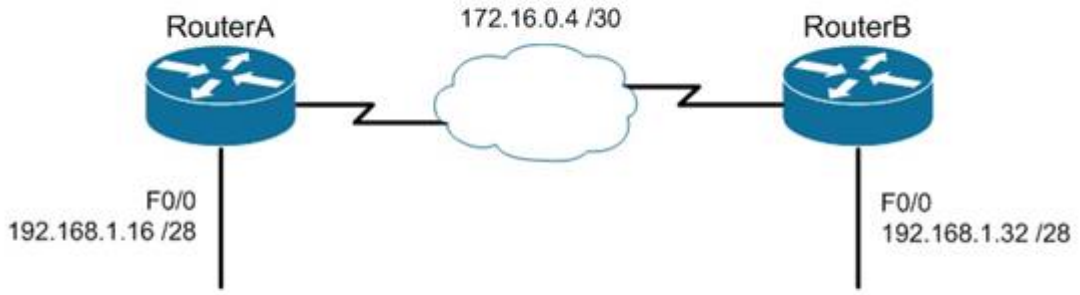
Cisco > Home > Support > Technology Support > IP > IP Addressing Services > Design > Design Technotes > NAT: Local and Global Definitions

Licensed to Berend Post berend.post@it-university.nl

Question 299

You are the Cisco administrator for Metroil. One of your assistants has submitted the given diagram as a potential addressing plan for two offices. Both offices use EIGRP as the routing protocol. You immediately see a problem with the proposal.

Which of the following actions could be a solution? (Choose two. Each correct option is a complete solution.)



- ☒ Execute the no auto-summary command on both routers.
- ☒ Change the network on F0/0 of Router A to 192.168.3.0/24 and change the network on F0/0 of Router B to 192.168.2.0/24.
- ☐ Change the network on F0/0 of Router B to 192.168.1.48/28.
- ☐ Execute the auto-summary command on both routers.

Explanation:

Explanation:

You should either execute the no auto-summary command on both routers, or change the network on F0/0 of Router A to 192.168.3.10/24 and the network on F0/0 of Router B to 192.168.2.0/24. The exhibit is an example of discontiguous subnets, in which two subnets (192.168.1.16 and 192.168.1.32) of the same major network (192.168.1.0) are separated by a completely different network (172.16.0.4/30). The no auto-summary command instructs EIGRP to stop automatically summarizing advertised networks to their classful boundaries. Without the no auto--summary command, EIGRP will automatically summarize these two subnets to 192.168.1.0, and advertise the summary route across the WAN link, losing the subnet-specific information and causing routing problems. The no auto-summary command stops this behavior, and allows EIGRP to advertise specific subnets.

An alternate solution would be to change the network on F0/0 of Router A to 192.168.3.0/24 and the network on F0/0 of Router B to 192.168.2.0/24. If that were done, the two networks would be in separate class C networks and auto summarization would not be a problem.

Licensed to Berend Post berend.post@it-university.nl

It would not help to change the network on F0/0 of Router B to 192.168.1.48/28. The two networks would still be in the same class C network and the summarization process would confuse routing.

It would not help to execute the auto-summary command. The command is already in effect by default.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Home > Support > Technology Support > IP > IP Routing >Technology Information>Technology White Paper> Enhanced Interior Gateway Routing Protocol> Auto-Summarization

Question 300

Which of the following TCP port numbers is used by Simple Mail Transfer Protocol (SMTP)?

- ☐ 23
- ☐ 21
- ☐ 53
- ☐ 80
- ☐ 57
- ☒ 25

Explanation:

Explanation:

TCP port 25 is assigned to SMTP. SMTP is a Transmission Control Protocol (TCP)/ Internet Protocol (IP) protocol used to send and receive e-mail messages.

Important TCP port number assignments are as follows:

TCP port 23 is used by Telnet to allow remote logins.

TCP port 21 is assigned to File Transfer Protocol (FTP) for FTP control. FTP also uses port 20 to transmit FTP data.

TCP and User Datagram Protocol (UDP) port 53 is assigned to Domain Name Service (DNS), which is used to convert hostnames into Internet Protocol (IP) addresses.

 Licensed to Berend Post berend.post@it-university.nl

TCP port 80 is used by Hypertext Transfer Protocol (HTTP), which is the base for transferring Web pages over the Internet.

TCP port 57 is assigned to Mail Transfer Protocol (MTP).

TCP port 22 is used by Secure Shell (SSH).

UDP ports 67 and 68 are used by Dynamic Host Configuration Protocol (DHCP).

UDP port 69 is used by Trivial FTP (TFTP).

TCP port 110 is used by Post Office Protocol 3 (POP3).

UDP port 161 is used by Simple Network Management Protocol (SNMP).

TCP port 443 is used by Secure Sockets Layer (SSL).

TCP port numbers help to direct data to the appropriate application, service, or application window. TCP port numbers ensure that data is displayed in the correct browser window when accessing Web data from multiple sources, and ensures it is directed to the proper application or service when received.

Objective:

Infrastructure Security

Sub-Objective:

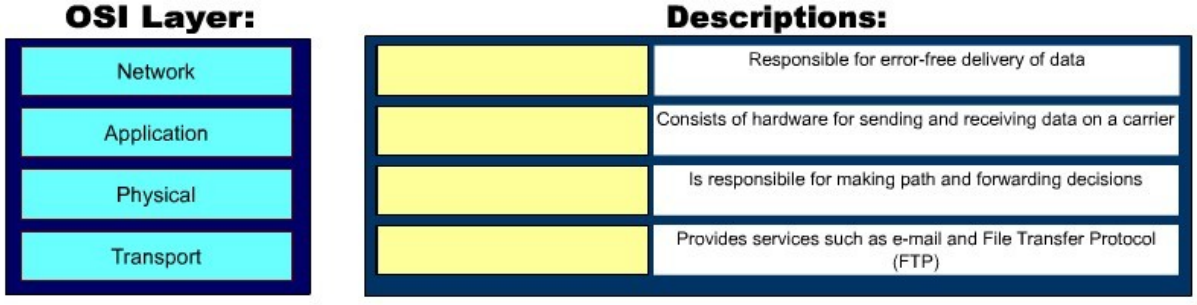
Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering

References:

Internetworking Technology Handbook > Internetworking Basics > OSI Model and Communication Between Systems>Multiplexing Basics

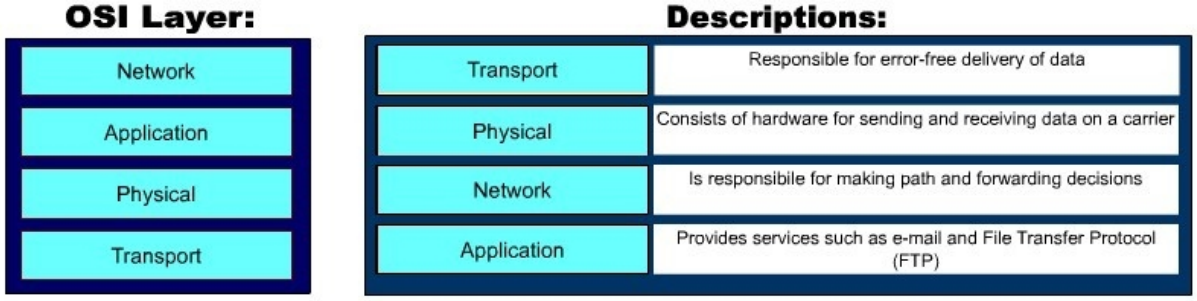
Question 301

DRAG DROP
Click and drag the Open Systems Interconnection (OSI) layers to their corresponding functions on the right.



 Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl

Question 302

Which Cisco IOS command is used on a Catalyst 2950 series switch to verify the port security configuration of a switch port?

- ☐ show interfaces port-security
- ☒ show port-security interface
- ☐ show ip interface
- ☐ show interfaces switchport

Explanation:

Explanation:

The show port-security interface command displays the current port security and status of a switch port, as in this sample output:

```
Switch# show port-security interface fastethernet0/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 2
Total MAC Addresses: 2
Configured MAC Addresses: 2
Aging Time: 30 mins
Aging Type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

The sample output indicates that port security has been enabled on interface FastEthernet0/1, and that a maximum of two MAC addresses has been configured. A violation policy of Shutdown indicates that if a third MAC address attempts to make a connection, the switch port will be disabled.

The violation mode setting has three possible values that take the following actions when a violation occurs:

protect Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.

restrict Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment. It will send a Syslog message and an SNMP trap as well.

 Licensed to Berend Post berend.post@it-university.nl

shutdown Puts the interface into the error-disabled state immediately and sends an SNMP trap notification

The show ip interface command is incorrect because it displays protocol-related information about an interface, and nothing pertaining to switch port security.

The show interfaces switchport command is incorrect because it displays non-security related switch port information, such as administrative and operational status and trunking.

The show interfaces port-security command is incorrect because this is not a valid Cisco command.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

Question 303

Which of the following is NOT managed by the cloud provider in an IaaS deployment?

- ☐ virtualization
- ☐ servers
- ☐ storage
- ☒ operating system

Explanation:

Explanation:

Operating systems are not managed by the cloud provider in an Infrastructure as a service (IaaS) deployment. Only storage, virtualization, servers, and networking are the responsibility of the provider. The customer is responsible for the following with IaaS:

Operating systems

Data

Applications

Middleware

Runtime

Licensed to Berend Post berend.post@it-university.nl

In a Platform as a Service (PaaS) deployment, the provider is responsible for all except the following, which is the responsibility of the customer:

Applications

Data

In Software as a Service (SaaS) deployment, the provider is responsible for everything.

Objective:

Network Fundamentals

Sub-Objective:

Describe the effects of cloud resources on enterprise network architecture

References:

IaaS, PaaS, SaaS (Explained and Compared)

Question 304

Which settings represent the proper BITs per second, data bits, and parity settings for a HyperTerminal session to the router?

- ☐ 19200,8,none
- ☒ 9600,8,none
- ☐ 9600,8, even
- ☐ 19200,8,even

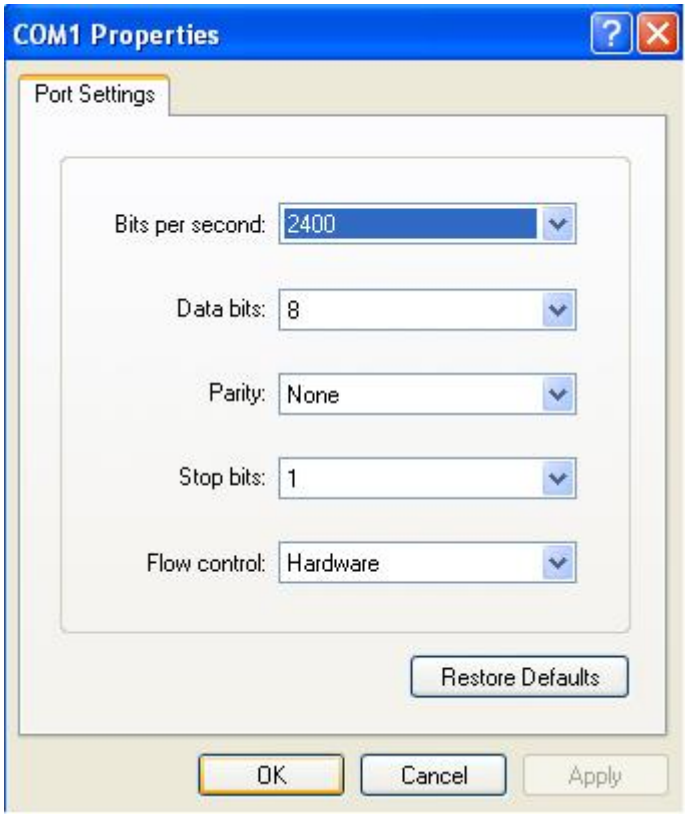
Explanation:

Explanation:

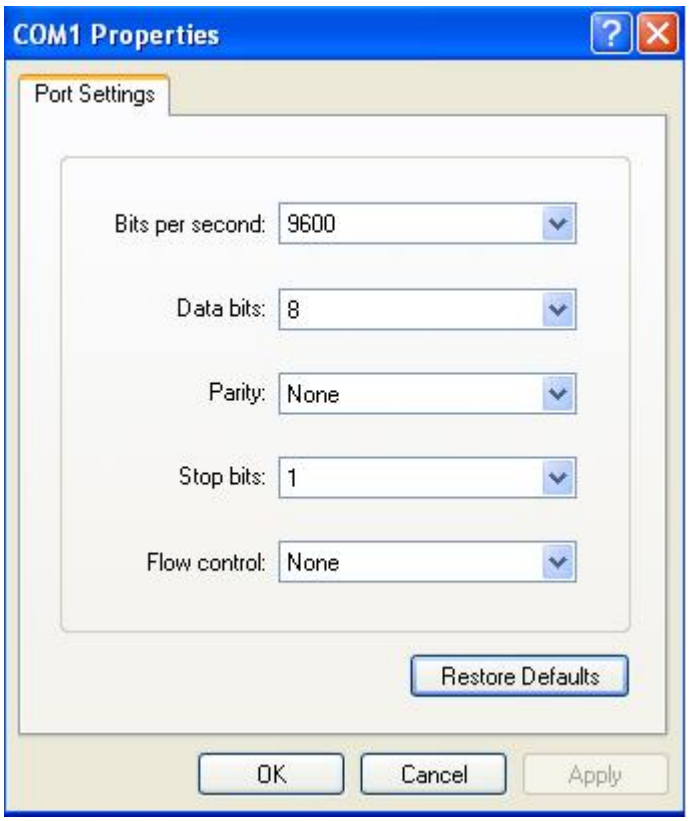
When setting up a HyperTerminal session to either a router or a switch, the proper settings must be enabled or the connection will not work. The proper settings are 9600 bits per second, 8 data bits, and none in the parity box. The HyperTerminal application is provided on Windows operating systems up to Windows XP. The path to the tool is Start > Programs > Accessories > Communications > HyperTerminal. For later Windows operating systems, a HyperTerminal program must be downloaded and installed.

After opening the tool, you will name the connection and select a COM port if you want to use a port other than the default, which is the serial port to which the console cable is connected. You will then be presented with the following box:

 Licensed to Berend Post berend.post@it-university.nl



The settings should reflect 9600 bits per second, 8 data bits, no parity, 1 stop bit, and no flow control, as illustrated in this graphic:



All other options include incorrect settings in at least one category.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device management

References:

Question 305

Which two fields are present in the output of the show ip interface brief command? (Choose two.)

- ☐ YES?
- ☐ Helper address
- ☒ OK?
- ☒ Method
- ☐ Proxy ARP

Explanation:

Explanation:

Sample output of the show ip interface brief command is as follows:

Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol

Ethernet0 10.108.00.5 YES NVRAM up up

Ethernet1 unassigned YES unset administratively down down

Loopback0 10.108.200.5 YES NVRAM up up

Serial0 10.108.100.5 YES NVRAM up up

Serial1 10.108.40.5 YES NVRAM up up

Serial2 10.108.100.5 YES manual up up

Serial3 unassigned YES unset administratively down down

The following fields are present in the output of the show ip interface brief command:

OK?: If the value of this field is "yes", it represents that the IP address is valid. If the value of this field is "No", it represents an invalid IP address.

Method: This field can have one of the following values:

 Licensed to Berend Post berend.post@it-university.nl

RARP or SLARP: Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request

BOOTP: Bootstrap protocol

TFTP: Configuration file obtained from TFTP server

Manual: Manually changed by CLI command

NVRAM: Configuration file in NVRAM

IPCP: ip address negotiated command

DHCP: ip address dhcp command

unassigned: No IP address

unset: Unset

other: Unknown

Interface: Refers to the type of interface.

IP-Address: Refers to the IP address assigned to the interface.

Status: Displays the interface status. Possible values in this field are as follows:

up: Interface is administratively up.

down: Interface is down.

administratively down: Interface is administratively down.

Protocol: An indicator of the operational status of the routing protocol for this interface.

YES? is not a valid field in the output of the show ip interface brief command.

Helper address and Proxy ARP fields are present in the output of the show ip interface command, not the show ip interface brief command.

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

 Licensed to Berend Post berend.post@it-university.nl

Cisco > Cisco IOS IP Addressing Command Reference > show ip interface

Question 306

Which Cisco IOS command can be used to troubleshoot switch startup problems on a Cisco Catalyst 2950 switch?

- ☐ show test
- ☐ show diagnostic
- ☒ show post
- ☐ show switchstartup

Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl

```
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 Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Cisco>Home>Support>Product Support>End-of-Sale and End-of-Life Products>Cisco Catalyst 6000 Series Switches>Troubleshoot and Alerts> Troubleshooting TechNotes> Troubleshooting Switch Port and Interface Problems> Most Common Port and Interface Troubleshooting Commands for CatOS and Cisco IOS

Cisco Documentation > Catalyst 3550 Multilayer Switch Hardware Installation Guide, Dec 2002 > Understanding POST Results

 Licensed to Berend Post berend.post@it-university.nl

Question 307

You are the network administrator for your company. You have implemented VLAN Trunking Protocol (VTP) in your network. However, you have found that VTP is not synchronizing VLAN information.

Which of the following items should be verified to resolve the problem? (Choose three.)

- ☐ Ensure that switches in the VTP domain are configured with VTP version 1 and version 2.
- ☐ Ensure that VLANs are active on at least one switch on the VTP domain.
- ☒ Ensure that all of the ports that interconnect switches are configured as trunks and are trunking properly.
- ☒ Ensure that the VTP domain name is the same on all switches in the domain.
- ☒ Ensure that identical passwords are configured on all VTP switches.

Explanation:

Explanation:

The following is a list of the steps to take if VTP fails to exchange VLAN information:

Ensure that all of the ports that interconnect switches are configured as trunks and are trunking properly.

Ensure that VLANs are active in all the devices.

Ensure that at least one switch is acting as a VTP server in the VTP domain.

Ensure that the VTP domain name is the same for all switches in the domain. The VTP domain name is case-sensitive.

Ensure that the VTP password is the same for all switches in the domain.

Ensure that the same VTP version is used by every switch in the domain. VTP version 1 and version 2 are not compatible on switches in the same VTP domain.

You should not ensure that switches are configured with VTP version 1 and version 2 in the domain, because VTP version 1 and version 2 are incompatible. VTP version 1 is the default on all Cisco switches.

You should not ensure that VLANs are active on at least one switch in the VTP domain, because VLANs should be active in all of the devices in a VTP domain.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

Licensed to Berend Post berend.post@it-university.nl

References:

Question 308

Which of the following IPV6 commands is used to define a static host name-to-address mapping in the host name cache?

- ☒ ipv6 host
- ☐ ipv6 unicast routing
- ☐ ipv6 neighbor
- ☐ ipv6 local

Explanation:

Explanation:

The ipv6 host command is used to define a static host name-to-address mapping in the host name cache, and is executed in global configuration mode.

The ipv6 unicast-routing command is used to enable IPv6 forwarding on a router.

There is no ipv6 local command. There is an ipv6 local pool command that can be used to define a prefix pool when using DHCPv6.

The ipv6 neighbor command is used to configure a static entry in the IPv6 neighbor discovery cache, which will enhance the neighbor discovery process that occurs with IPv6.

Objective:

Infrastructure Services

Sub-Objective:

Troubleshoot client connectivity issues involving DNS

References:

Cisco > Cisco IOS IPv6 Command Reference > ipv6 host

Licensed to Berend Post berend.post@it-university.nl

Question 309

Which of the following represents the correct method of assigning an IP address and default gateway to a switch?

- ☐ Switch(config)# interface vlan1
- ☐ Switch(config-if)# ip address 10.0.0.1 255.0.0.0
- ☐ Switch(config-if)# default-gateway 10.0.0.254
- ☒ Switch(config)# ip default-gateway 10.0.0.254
- ☒ Switch(config)# interface vlan1
- ☒ Switch(config-if)# ip address 10.0.0.1 255.0.0.0
- ☐ Switch(config)# ip address 10.0.0.1 255.0.0.0
- ☐ Switch(config)# default-gateway 10.0.0.254
- ☐ Switch(config)# ip address 10.0.0.1 255.0.0.0
- ☐ Switch(config)# interface vlan1
- ☐ Switch(config)# ip default-gateway 10.0.0.254

Explanation:

Explanation:

IP addresses are assigned to switches by assigning the address to VLAN 1 using the ip address command, while the default gateway is configured in global configuration mode using the ip default-gateway command. A default gateway is assigned to a Layer 2 switch using the following command syntax, where h.h.h.h is the IP address of the default gateway:

Switch(config)# ip default-gateway h.h.h.h

An IP address is assigned to a Layer 2 switch using the following command syntax, where h.h.h.h is the IP address and m.m.m.m is the subnet mask:

Switch(config)# interface vlan1

Switch(config-if)# ip address h.h.h.h m.m.m.m

Configuring an IP address on a switch is usually accompanied by adding a default gateway as well. Switches do not require an IP address to perform their function on the network. IP addresses are added so that an administrator can make a Telnet connection to the switch to manage the switch. If this Telnet access does not occur on the same local subnet with the switch, which is unlikely, or if the administrator is trying to Telnet to the switch using a host that resides a VLAN other VLAN1 (the management VLAN) the absence of a gateway address will render the switch incapable of answering Telnet connection attempts. Therefore, a gateway address is usually required on the switch to make a telnet connection.

Licensed to Berend Post berend.post@it-university.nl

The following command set is incorrect because the command setting the default gateway must be executed in global configuration mode, not in configuration mode, for VLAN1:

Switch(config)# interface vlan1

Switch(config-if)# ip address 10.0.0.1 255.0.0.0

Switch(config-if)# default-gateway 10.0.0.254

The following command set is incorrect because the IP address must be configured in configuration mode for VLAN1, not global configuration mode:

Switch(config)# ip address 10.0.0.1 255.0.0.0

Switch(config)# default-gateway 10.0.0.254

The following command set is incorrect because an IP address must be configured in configuration mode for VLAN1. Also, if you executed the command interface vlan1, the prompt would change to Switch(config-if)#. Once it did, that would be an incorrect mode for entering the default gateway.

Switch(config)# ip address 10.0.0.1 255.0.0.0

Switch(config)# interface vlan1

Switch(config)# ip default-gateway 10.0.0.254

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device management

References:

Licensed to Berend Post berend.post@it-university.nl

Question 310

Which statements are NOT true regarding Virtual Local Area Networks (VLANs)? (Choose two.)

- ☐ VLANs define broadcast domains.
- ☐ VLANs are logical groups of hosts.
- ☒ VLANs are location-dependent.
- ☒ VLANs are limited to a single switch.
- ☐ VLANs may be subnets of major networks.

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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/extended range) spanning multiple switches

References:

Question 311

You are the network administrator for your company. You want to implement a routing protocol that can support hierarchical routing, multiple vendor environments, and authentication, and provides fast convergence.

Which routing protocol will you implement?

- ☐ Enhanced Interior Gateway Routing Protocol (EIGRP)
- ☒ Open Shortest Path First (OSPF)
- ☐ Routing Information Protocol version 2 (RIPv2)
- ☐ Interior Gateway Routing Protocol (IGRP)

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Open Shortest Path First (OSPF) is the routing protocol that accomplishes this task. The following are characteristics of OSPF:

Conveges very quickly.

Uses cost to detemine the best route.

Uses Internet Protocol (IP) protocol 89.

Has a default administrative distance of 110.

Is an industry standard protocol (non Cisco-proprietary).

Supports Non-Broadcast Multi-Access (NBMA) networks such as frame relay, X.25, and Asynchronous Transfer Mode (ATM). The default hello interval for NBMA networks is 30 seconds.

Supports point-to-point and point-to-multipoint connections.

Supports authentication.

Uses 224.0.0.6 as multicast address for ALLDRouters.

Uses 224.0.0.5 as multicast address for ALLSPFRouters.

Uses link-state updates and SPF calculation that provides fast convergence.

Recommended for large networks due to good scalability.

Uses cost as the default metric.

Supports VLSM.

Create minimal overhead due to its hierarchical design.

In OSPF networks, a hierarchical IP addressing design and the use of areas yields the following benefits:

Faster convergence

Reduced routing overhead

Confinement of network instability to a single area of the network

Electing a designated router (DR) in each area reduces update traffic because all updates occur through the DR. The DR election is based on the router ID. This is the highest IP address of the active interfaces when no loopback interface is configured. When a loopback address is present, its address is used for the purposes of DR election. In either case, the router with highest router ID becomes the DR.

EIGRP and IGRP are incorrect because they are Cisco-proprietary routing protocols, and thus do not support multiple vendor environments. They also do not support hierarchical routing. IGRP is no longer being supported by Cisco.

 Licensed to Berend Post berend.post@it-university.nl

RIPv2 is incorrect because it does not support hierarchical routing or provide fast convergence.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

Cisco > Articles > Cisco Certification > CCNP > Shooting Trouble with IP

Cisco > Internetworking Technology Handbook > Open Shortest Path First (OSPF)

Question 312

Which of the following is NOT a characteristic of private Internet Protocol (IP) addressing?

- ☐ These addresses are not routable through the public Internet.
- ☒ These addresses are publicly registered with the Internet Network Information Center (InterNIC).
- ☐ These addresses are reserved by the Internet Assigned Numbers Authority (IANA).
- ☐ The ranges of private IP addressing are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.

Explanation:

Explanation:

It is NOT correct to state that private IP addresses are publicly registered with the Internet Network Information Center (InterNIC). Only public IP addresses are registered with the InterNIC.

The following characteristics are TRUE regarding private IP addressing:

Private addresses are not routable through the public Internet.

Private addresses are reserved by the Internet Assigned Numbers Authority (IANA).

The ranges of private IP addressing are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255.

The use of private IP addressing conserves the use of the public IPv4 address space

Private addresses cannot be registered publicly.

Private IP addresses conserve public addressing space and can improve network security.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Network Fundamentals

Sub-Objective:

Describe the need for private IPv4 addressing

References:

Question 313

What is the possible IP range that can be assigned to hosts on a subnet that includes the address 192.168.144.34/29?

- ☐ 192.168.144.32 - 192.168.144.63
- ☒ 192.168.144.33 - 192.168.144.38
- ☐ 192.168.144.33 - 192.168.144.48
- ☐ 192.168.144.28 - 192.168.144.40

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

We can stop at the 192.168.144.40 address because the address given in the scenario, 192.168.144.34, is in the network with a subnet ID of 192.168.144.32. Therefore, since the broadcast address for this network will be 1 less than the next subnet ID (192.168.144.39), the valid range of IP addresses is 192.168.144.33 - 192.168.144.38. 192.168.144.39 will be the broadcast address for the next subnet, and 192.168.144.40 will be the first valid address in the next subnet.

None of the other answers is the correct range.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Question 314

You would like for Router25 in your OSPF network to become the DR. You execute the show ip ospf interface command, receiving the output shown below.

```
Router25# show ip ospf interface
Ethernet0 is up, line protocol is up
Internet Address 10.10.10.1/24, Area 0
Process ID 1,Router ID 10.10.10.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 172.16.10.1, Interface address 10.10.10.2
Backup Designated router(ID)10.10.10.1,Interface address 10.10.10.1
<output omitted>
```

You assign an IP address of 192.168.5.6 to the Ethernet1 interface of Router25 and enable the interface. However, Router25 does NOT become the designated router.

What additional command must you execute to cause Router25 to become the DR?

- ☒ Router25(config-router)# network 192.168.5.0 0.0.0.255 area 0
- ☐ Router25(config-router)# network 192.168.5.0 0.0.0.255 area 1
- ☐ Router25(config-router)# network 192.168.5.0 255.255.255.0 area 0
- ☐ Router25(config)# network 192.168.5.0 0.0.0.255 area 0

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The command Router25(config-router)# network 192.168.5.0 0.0.0.255 area 0 must be executed to enable Router25 to become the DR. For an interface to be considered in the DR election, it must be advertised in OSPF. Otherwise, it is not participating in OSPF routing and you may be faced with the situation illustrated by the output of the shown ip ospf interface command below:

```
Router25# show ip ospf interface
Ethernet0 is up, line protocol is up
Internet Address 10.10.10.1/24, Area 0
Process ID 1,Router ID 225.16.33.4, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 172.16.10.1, Interface address 10.10.10.2
Backup Designated router(ID)225.16.33.4,Interface address 10.10.10.1
<output omitted>
```

The RID of Router25, 225.16.33.4, is higher than that of the current DR, which has an RID of 172.16.10.1. Despite that fact, Router 25 did not become the DR because the 225.0.0.0 network has not been advertised. This could be verified by executing the show ip protocols command as shown below:

```
Router25# show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 225.16.33.4
<output omitted>

Routing for Networks:
10.0.0.0 0.0.0.255 area 0
```

As only the 10.0.0.0 network is being advertised, the 225.16.33.4 IP address will not be a factor in the DR election.

The command Router25(config-router)# network 192.168.5.0 0.0.0.255 area 1 is incorrect because it references area 1 instead of area 0, which is the area in use in this scenario.

The command Router25(config-router)# network 192.168.5.0 255.255.255.0 area 0 is incorrect because it uses a regular mask instead of a wildcard mask. Network commands in OSPF must use a wildcard mask.

The command Router25(config)# network 192.168.5.0 0.0.0.255 area 0 is incorrect because it is executed at the global configuration, router25(config)#, prompt rather than the OSPF configuration prompt, router25(config-router)#.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Cisco > Home > Support > Technology Support > IP > IP Routing > Technology Information > Technology White paper > OSPF Design Guide

Question 315

Which trunk encapsulation defines one VLAN on each trunk as a native VLAN?

- ☐ ISL
- ☒ IEEE 802.1q
- ☐ IEEE 802.11a
- ☐ auto

Explanation:

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.

 Licensed to Berend Post berend.post@it-university.nl

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:

Question 316

What is the Institute of Electrical and Electronics Engineers (IEEE) specification for Spanning Tree Protocol (STP)?

- ☒ 802.1d
- ☐ 802.1q
- ☐ 802.3u
- ☐ 802.3z

Explanation:

Explanation:

The IEEE specification for STP is 802.1d. STP uses the spanning-tree algorithm to find and prevent loops in redundant network topologies. This helps mitigate broadcast storms, multiple copies of frames, and Media Access Control (MAC) address database inconsistencies.

The IEEE committee developed the 802.1 series of specifications for bridging. The IEEE 802.1q specification is for Virtual LAN (VLAN) trunking. Per this specification, a 4-byte 802.q header, which contains the Priority and VLAN ID fields, is inserted in the middle of the original Ethernet header.

802.3 is the IEEE committee specification that defines the Ethernet group. Ethernet is a LAN protocol that specifies physical layer and MAC sublayer media access. IEEE 802.3 uses carrier sense multiple access collision detect (CSMA/CD) to provide access for many devices on the same network. 802.3u is the IEEE specification for Fast Ethernet. 802.3z is the IEEE specification for Gigabit Ethernet.

Objective:

 Licensed to Berend Post berend.post@it-university.nl

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Support > Configuring Spanning Tree-Protocol > How STP Works

Question 317

What Cisco IOS command produced the following as a part of its output?

Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 2
Total MAC Addresses: 2
Configured MAC Addresses: 2
Aging Time: 30 mins
Aging Type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0

- ☐ show interfaces port-security
- ☒ show port-security interface
- ☐ show ip interface
- ☐ show interfaces switchport

Explanation:

Explanation:

The output is the result of executing the show port-security interface command. The sample output indicates that port security has been enabled on the interface, and that a maximum of two MAC addresses has been configured. A violation mode of Shutdown indicates that if a third MAC address attempts to make a connection, the switch port will be disabled. It is useful to note that you must specify a port number when you execute the command. In this case, the command was Switch# show port-security interface fastethernet0/1.

The output was not produced by the show interfaces port-security command. This is not a valid Cisco command.

The output was not produced by the show ip interface command. It displays protocol-related information about an interface, and nothing pertaining to switch port security. An example of its output follows:

 Licensed to Berend Post berend.post@it-university.nl

```
Router# show ip interface fastethernet0/1
fastethernet0/1 is up, line protocol is up
Internet address is 10.1.1.1/16
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN Flow CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is enabled, using route map PBR
Network address translation is disabled
BGP Policy Mapping is disabled
IP Multi-Processor Forwarding is enabled <======== MPF information
IP Input features, "PBR",
are not supported by MPF and are IGNORED
IP Output features, "NetFlow",
are not supported by MPF and are IGNORED
```

The output was not produced by the show interfaces switchport command. This command displays non-security related switch port information, such as administrative and operational status and trunking:

Licensed to Berend Post berend.post@it-university.nl

```
Cat2950# show interfaces fastethernet0/1 switchport
Name: Po1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Voice VLAN: none (Inactive)
Appliance trust: none
```

Objective:

Infrastructure Security

Sub-Objective:

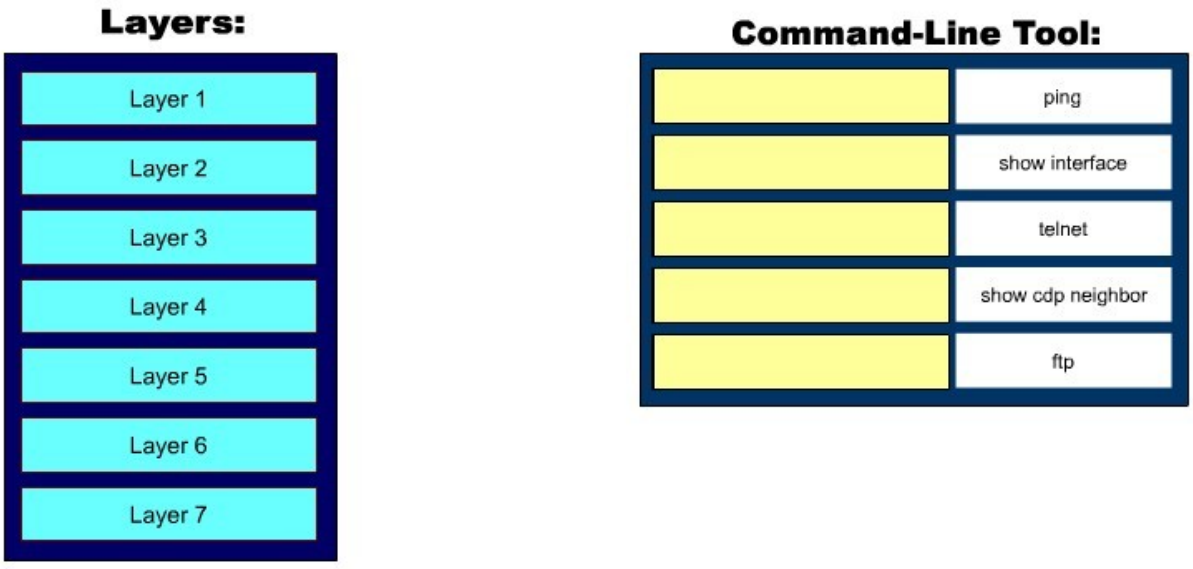
Configure, verify, and troubleshoot port security

References:

Cisco > Support > Cisco IOS Security Command Reference: Commands S to Z > show port-security

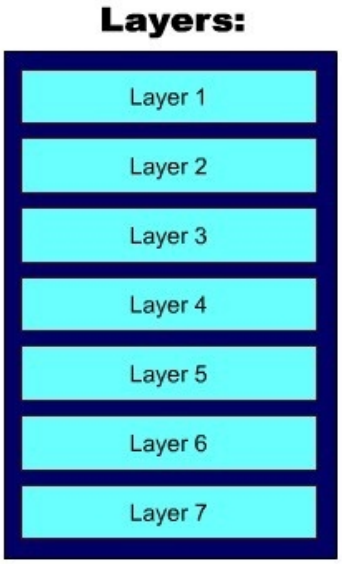
Question 318

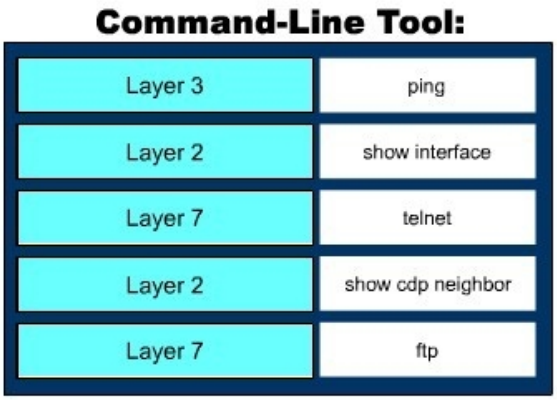
DRAG DROP
Click and drag the OSI layer, on the left, to the commands at which they test functionality. If a command can test more than one layer, choose the highest layer for which it can test. (It may be necessary to use an OSI layer multiple times.)



Licensed to Berend Post berend.post@it-university.nl

Solution:





Explanation:

Explanation:

Telnet operates at the application layer, which is Layer 7 of the OSI model. File transfer Protocol (FTP) is a generic command that is also used by some high-end Cisco routers but in a different format. FTP also operates at Layer 7. The ping command operates at the network layer, which is Layer 3 of OSI reference model. Therefore, it is used to test the connectivity up to Layer 3. The show interface command will display the status of line protocol. If it displays the message interface up, line protocol up it means that Layer 2 is functioning correctly.

The show cdp neighbor command also operates at Layer 2, which is the data link layer.

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

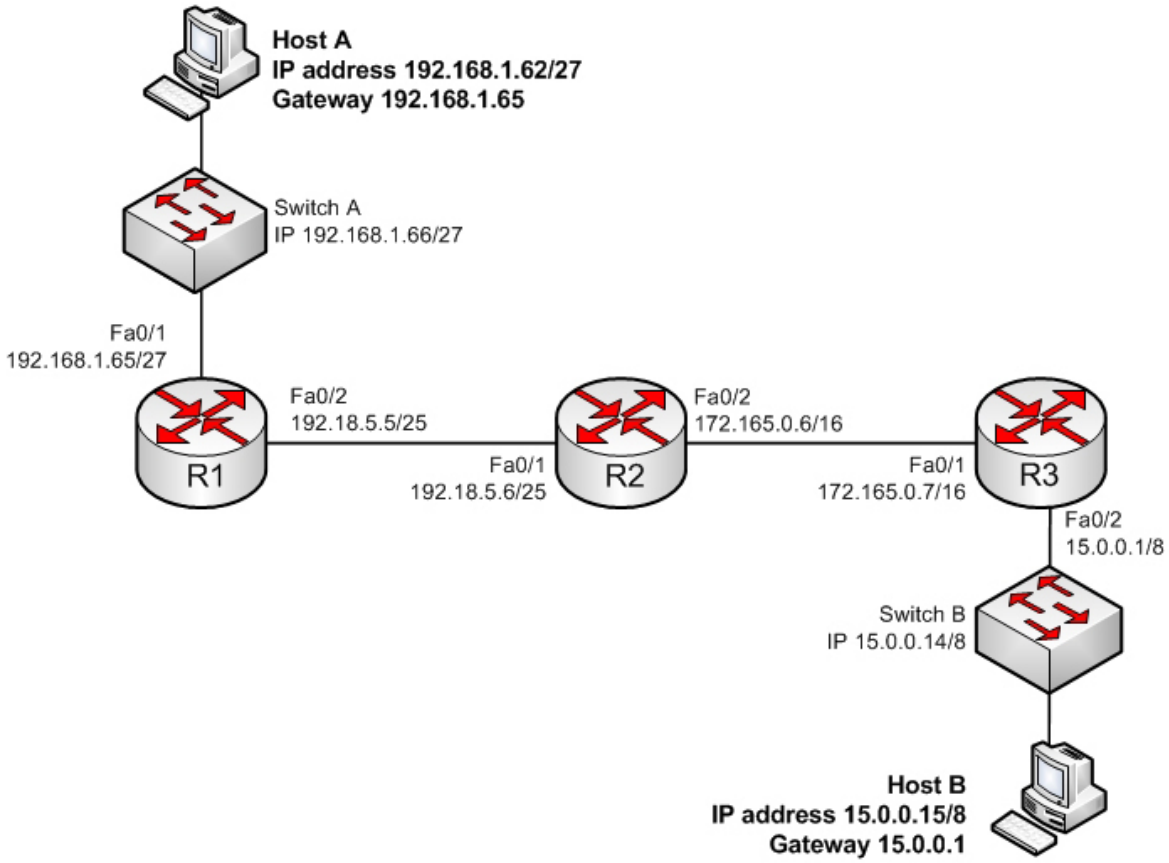
References:

Cisco Documentation > Internetworking Technology Handbook > Internetworking Basics > OSI model

Licensed to Berend Post berend.post@it-university.nl

Question 319

Examine the diagram below and assume that routing is configured properly.



Why is Host A unable to ping Host B?

- ☐ The IP address of Switch A is incorrect
- ☐ The gateway address of Host B is incorrect
- ☒ The IP address of Host A is incorrect
- ☐ The Fa0/2 and Fa0/1 interfaces on R1 and R2 are not in the same subnet

Explanation:

Explanation:

The IP address of Host A is incorrect. The Fa0/1 interface on R1 (Host A's default gateway) is in the 192.168.1.64/27 network, and Host A's IP address is in the 192.168.1.32/27 network. With a 27-bit mask against the 192.168.1.0 classful network, the resulting subnets are:

192.168.1.0

192.168.1.32

192.168.1.64

192.168.1.92

Licensed to Berend Post berend.post@it-university.nl

And so it would continue, increasing the fourth octet in intervals of 32. By only going this far we can see that they are in different subnets.

The IP address of Switch A is correct for its subnet because it needs to be in the same subnet as the Fa0/1 interface on R1. Even if it were incorrect or missing altogether it would have no impact on Host A. Switches merely switch frames based on MAC addresses and only need an IP address for management purposes.

The gateway address of Host B is correct. It is in the same subnet (15.0.0.0/8) with the Fa0/2 interface on R2, its gateway.

The Fa0/2 and Fa0/1 interfaces on R1 and R2 are in the same subnet. Using a 25-bit mask against the 192.18.5.0/24 classful network yields the following subnets:

192.18.5.0

192.168.5.128

Both router interfaces in question are in the 192.18.5.0 subnet.

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Cisco > Support > IP Routing > Design TechNotes > Document ID: 13788 > IP Addressing and Subnetting for New Users

Question 320

Which of the following commands would allow you to determine the bandwidth of an interface?

- ☒ show interfaces
- ☐ show interfaces accounting
- ☐ show cdp
- ☐ show cdp neighbors

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The show interfaces command shows information about each interface including a section on the bandwidth of the connection. If you wanted to locate this information in the output, it would be in the third down line as follows:

MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255

Where BW = bandwidth

The show interfaces accounting command focuses on the relative amounts of traffic going through each interface, but does not indicate the bandwidth.

The show cdp command shows information about the Cisco Discovery protocol, a Layer 2 protocol used by Cisco devices to advertise their existence and capabilities to other Cisco devices ion the network.

The show cdp neighbors command shows information about each discovered neighbor, but does not display the bandwidth of an interface.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Question 321

Which of the following statements is NOT true of Cisco ACI?

- ☐ It is a comprehensive SDN architecture.
- ☐ It uses Cisco APIC as the central management system.
- ☐ It provides policy driven automation support.
- ☒ It decreases network visibility.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The Cisco ACI does not decrease network visibility. On the contrary, the Cisco Application Centric Infrastructure (ACI) increases network visibility. It is a policy-driven automaton solution that can keep the network inventory up-to-date automatically whenever a new device is added and provide a graphic representation at all times.

ACI is a comprehensive SDN architecture that integrates physical and virtual environments under one policy model. It uses the Cisco Application Policy Infrastructure Controller (APIC) as the central management system.

It provides policy driven automation support through a business-relevant application policy language.

Objective:

Infrastructure Management

Sub-Objective:

Describe network programmability in enterprise network architecture

References:

Home > Support > Product Support > Cloud and Systems Management > Cisco Application Policy Infrastructure Controller (APIC) > Reference Guides > Technical References Cisco Application Centric Infrastructure Fundamentals

Question 322

Which statement correctly identifies a difference between Inter-Switch Link (ISL) and 802.1q?

- ☒ 802.1q uses a native VLAN, ISL does not.
- ☐ Cisco devices support only ISL.
- ☐ ISL uses a 12-bit VLAN number field, and 802.1q does not.
- ☐ ISL modifies the original Ethernet frame, while 802.1q encapsulates the original Ethernet frame.

Explanation:

Explanation:

802.1q defines a native virtual LAN (VLAN) on each trunk link, which defaults to VLAN 1. The 802.1q frame tagging method specifies that frames in the native VLAN will not be tagged while transmitting over a trunk link. The switch on the other end of the link identifies a native VLAN frame by the absence of the 802.1q header. ISL does not have the concept of native VLANs, and traffic from all VLANs is encapsulated.

Licensed to Berend Post berend.post@it-university.nl

While older Cisco devices support both the ISL and 802.1q frame tagging methods, ISL is a deprecated, Cisco-proprietary frame tagging method, and newer Cisco switches only support the 802.1q standard. When switches from multiple vendors are installed in the network, the 802.1q frame tagging method should be used.

It is incorrect to state that ISL uses a 12-bit VLAN number field and 802.1q does not. ISL uses a 15-bit VLAN ID field, while 802.1q uses a 12-bit VLAN ID field.

ISL encapsulates the original Ethernet frame, adding a 26-byte header and a 4-byte trailer. 802.1q operates by inserting a 4-byte header inside the original Ethernet frame, then recalculating the checksum (CRC) in the Ethernet trailer.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format > Document ID: 17056

Licensed to Berend Post berend.post@it-university.nl

Question 323

A switch that you manage has three VLANs configured. Its MAC address table is shown below:

Vlan Mac address Type Ports
<output omitted>
1 000f.e544.c2b3 dynamic Fa0/10
1 000d.4589.00b8 dynamic Fa0/5
1 00bd.000b.005bb dynamic Fa0/8
11 0001.0d44.bbdb dynamic Fa0/12
55 0014.0bd4.0054 dynamic Fa0/15
66 00bb.224b.0ac5 dynamic Fa0/1

You execute the following command on the switch:

Switch# show int trunk

Port mode Encapsulation Status Native VLAN
Fa0/10 on 802.1q trunking 1
Fa0/5 on 802.1q trunking 1
Fa0/8 on 802.1q trunking 1

Considering only the ports listed in the output, if a frame enters the switch untagged with a destination address of 0002.254b.0015, which ports will receive the frame? (Choose all that apply.)

- ☐ All ports
- ☐ Ports 5, 8, and 11
- ☐ All unaccounted-for access ports
- ☒ All ports in the same VLAN except the port on which it arrived
- ☒ All 802.1q trunk links

Explanation:

Explanation:

When a switch receives a frame, the first thing it will do is determine if the frame's MAC address is already in its MAC table. If it is not, as in this scenario, it will send the frame out on all access ports in the same VLAN and any 802.1q trunks with the exception of the port on which it arrived. Since the frame is untagged it will be in VLAN 1 by default.

In the MAC table shown in the output, there is no listing for the MAC address 0002.254b.0015. This indicates that the destination is not directly connected to this switch. Therefore, the switch will send the frame to all trunk links, which in this case would be ports 10, 5, and 8, and all access links in VLAN 1 with the exception of the one on which it arrived, which was not identified in the scenario.

Objective:

LAN Switching Fundamentals

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Describe and verify switching concepts

References:

Question 324

Which of the following IP addresses are valid Class B host addresses if a default Class B mask is in use? (Choose all that apply.)

- ☐ 10.6.8.35
- ☒ 133.6.5.4
- ☐ 192.168.5.9
- ☐ 127.0.0.1
- ☒ 190.6.5.4

Explanation:

Explanation:

The IP addresses 133.6.5.4 and 190.6.5.4 are both valid Class B addresses when a default mask is in use. The Class B default mask is 255.255.0.0 and the range of valid addresses is 128.0.0.0-191.255.255.255.

The IP address 10.6.8.35 is a Class A address. The Class A default mask is 255.0.0.0 and the range of valid addresses is 1.0.0.0 - 127.255.255.255, with the exception of the range 127.0.0.1 - 127.255.255.255, which is reserved and cannot be assigned.

The IP address 192.168.5.9 is a Class C address. The Class C default mask is 255.255.255.0 and the range of valid addresses is 192.0.0.0 - 223.255.255.255.

The IP address 127.0.0.1 is a Class A address, but it comes from a reserved portion that cannot be assigned. The range 127.0.0.1 - 127.255.255.255 is used for diagnostics, and although any address in the range will work as a diagnostic address, 127.0.0.1 is known as the loopback address. If you can ping this address, or any address in the 127.0.0.1 - 127.255.255.255 range, then the NIC is working and TCP/IP is installed. The Class A default mask is 255.0.0.0 and the range of valid addresses is 1.0.0.0 - 127.255.255.255, with the exception of the range 127.0.0.1 - 127.255.255.255, which is reserved and cannot be assigned.

Objective:

Network Fundamentals

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

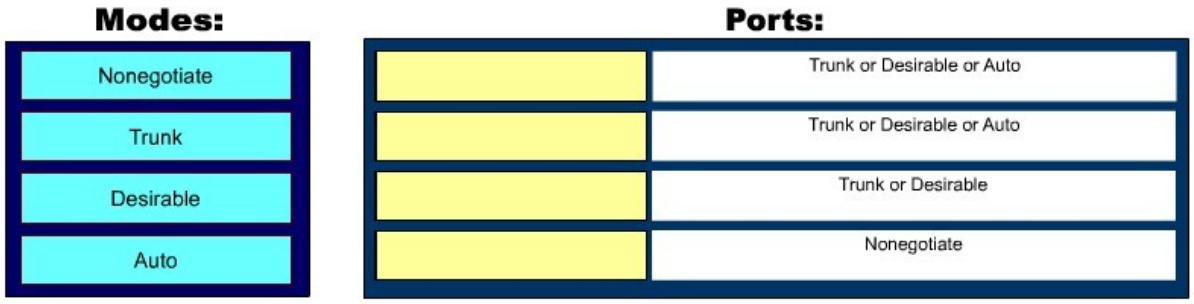
Compare and contrast IPv4 address types

References:

Cisco > Design Tech Notes > IP Routing > IP Addressing and Subnetting for New Users > Understanding IP Addresses > Document ID: 13788

Question 325

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.)



Solution:



Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

Objective:

LAN Switching Fundamentals

Sub-Objective:

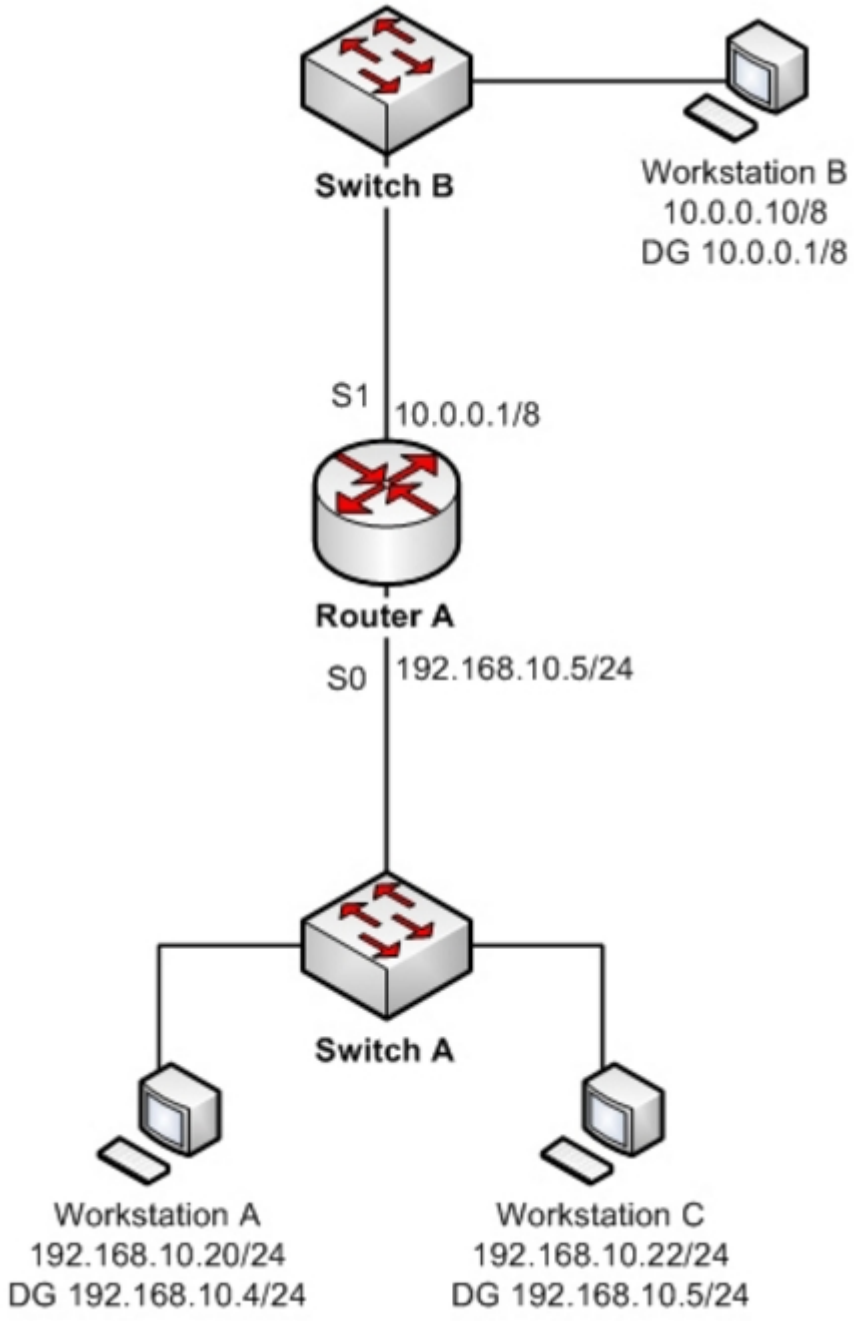
Configure and verify Layer 2 protocols

References:

Licensed to Berend Post berend.post@it-university.nl

Question 326

You are the Cisco administrator for Verigon Incorporated. The given exhibit displays some of the devices in the network. (Click the Exhibit(s) button.) Workstation A can communicate with Workstation C but cannot communicate with Workstation B.



What is the problem?

- ☐ Workstation B has an incorrect default gateway
- ☐ Workstation A has an incorrect subnet mask
- ☒ Workstation A has an incorrect default gateway
- ☐ Workstation B has an incorrect subnet mask

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Explanation:

Workstation A has an incorrect default gateway. To communicate with remote computers or those computers outside of its own subnet, a computer must have the address of the nearest router interface as its default gateway. In this case, the default gateway of Workstation A should be 192.168.10.5/24, which is the Serial0 address of Router A. The diagram shows that it is instead configured as 192.168.10.4/24. This will not cause a problem for Workstation A to communicate with Workstation C, but it will make communication with remote subnets impossible.

Workstation B does not have an incorrect default gateway. Its nearest router interface is 10.0.0.1/8, which is the configuration of its default gateway.

Workstation A does not have an incorrect subnet mask. The mask used by Workstation C and the router interface of Router A, which are in the same subnet, is /24, or 255.255.255.0, which is also the subnet mask used by Workstation A.

Workstation B does not have an incorrect subnet mask. Since the subnet mask of the router interface that is nearest to Workstation B is /8, or 255.0.0.0, then Workstation B also should have an 8-bit mask.

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

Cisco > Technology Support > IP > IP Routing > Design Technotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Cisco > Technology Support > IP > IP Addressing Services > Design Technotes > Subnet Zero and the All-Ones Subnet > Document ID: 13711

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Appendices D, E and H: Subnetting.

Licensed to Berend Post berend.post@it-university.nl

Question 327

Which two statements are TRUE of synchronous serial ports? (Choose two.)

- ☒ These ports can be used to provide leased-line or dial-up communications.
- ☐ These ports do not support the High-Level Data Link Control (HDLC) encapsulation method.
- ☐ An AUI connector is used with serial ports.
- ☒ These ports can be used to configure high-speed lines (E1 or T1).
- ☐ An RJ-45 connector is used with serial ports.

Explanation:

Explanation:

Synchronous serial ports can be used to provide leased-line or dial-up communications, and these ports can be used to configure high-speed lines (E1 or T1). The following are also true of synchronous serial ports:

With the help of synchronous serial lines, dialers can be configured, which are then used to support dial-on-demand routing.

These ports are found on several serial network interface processors and cards.

The option stating that synchronous serial ports cannot support High-Level Data Link Control (HDLC) encapsulation method is incorrect because HDLC is the default encapsulation method configured on serial interfaces.

The option stating that an AUI connector is used with serial ports is incorrect because AUI is a connector used with Ethernet ports.

The option stating that an RJ-45 connector is used with serial ports is incorrect because RJ-45 and RJ-48 connectors are used with ISDN BRI connections.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Licensed to Berend Post berend.post@it-university.nl

Question 328

A packet is received with a destination IP address of 10.2.16.10.

```
Router# show ip route
<<output omitted>>

D 10.0.0.0 /8 [90/2172515] via 192.168.1.10, 00:00:44, Serial0/0
D 10.1.0.0 /16 [90/2144425] via 192.168.1.10, 00:01:03, Serial0/0
C 192.168.1.0 is directly connected, Serial0/0
C 192.168.4.0 is directly connected, Serial0/1
D 10.2.16.0 /24 [90/2162425] via 192.168.4.2, 00:00:25, Serial0/1
C 192.168.10.0 is directly connected, Serial1/0
D 10.2.32.0 /24 [90/2172425] via 192.168.10.254, 00:00:21, Serial1/0
          90/2172425] via 192.168.1.10, 00:03:33:, Serial0/1
```

What would the next hop IP address be for this packet?

- ☐ 192.168.1.10
- ☒ 192.168.4.2
- ☐ 192.168.10.254
- ☐ None; the packet will be dropped.

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

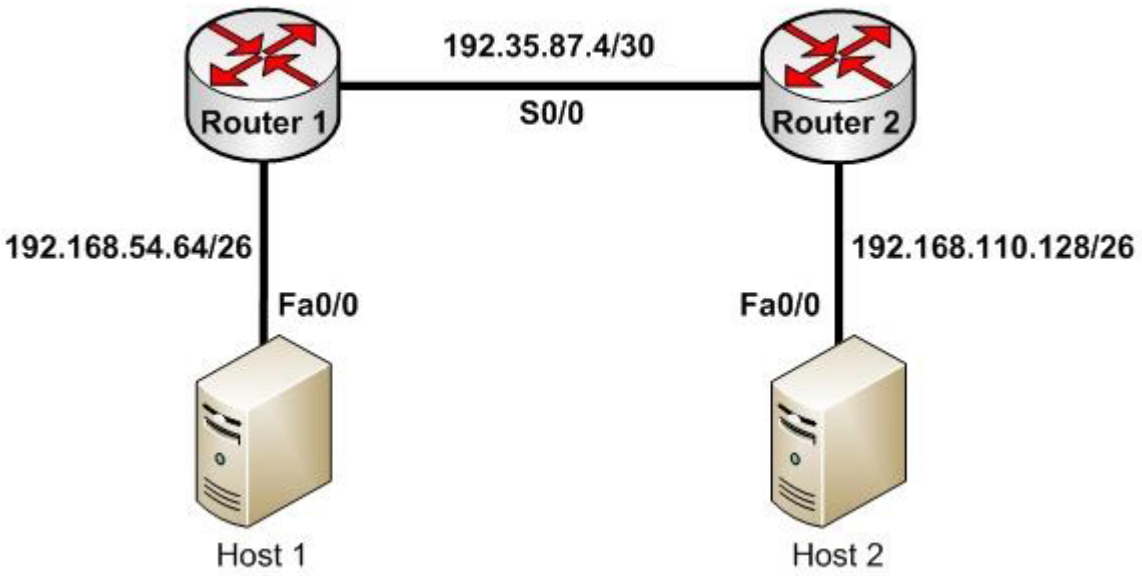
The packet will not be dropped because there is at least one routing table entry that matches the destination IP address of the packet.

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:



Licensed to Berend Post berend.post@it-university.nl

```
hostname router 1       hostname router 2
router rip                              router rip
network 192.168.54.64                 network 192.168.110.128
ip route 0.0.0.0 0.0.0.0 192.35.87.5 <output omitted> <output omitted>
```

Based on this output and diagram, we can reconstruct the contents of the routing table for Router 1 as follows.

```
S*0.0.0.0/0 [1/0] via 192.35.87.5
R 192.168.110.128/26 [120/1] via 192.35.87.5 00:00:22, Serial 0/0
C 192.35.87.4/30 is directly connected, S0/0
C 192.168.54.64/26 is directly connected, Fa0/0
```

It will contain S*0.0.0.0/0 [1/0] via 192.35.87.5 because of the static default route indicated in line 4 of its configuration output.

It will contain R 192.168.110.128/26 [120/1] via 192.35.87.5 00:00:22, Serial 0/0 because Router 2 has a network 192.168.110.128 statement indicating that it will advertise this network to its neighbors.

It will contain the two routes C 192.35.87.4/30 is directly connected, S0/0 and C 192.168.54.64/26 is directly connected, Fa0/0 because all directly connected routes are automatically placed in the table.

Objective:

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Cisco > Support > IP > IP Routing > Design > Design TechNotes > Route Selection in Cisco Routers > Document ID: 8651

Question 329

On Cisco switches, what is the correct order of port transition through the Spanning Tree Protocol (STP) states?

- ☐ learning, listening, blocking, forwarding
- ☐ listening, blocking, forwarding, learning
- ☐ blocking, learning, forwarding, listening
- ☒ blocking, listening, learning, forwarding

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

There are five states in STP transition:

Blocking

Listening

Learning

Forwarding

Disabled

After STP initialization, a port moves from blocking to listening, then to learning, and finally into forwarding state. In case of any errors or exceptions, a port may enter into a disabled state directly from any of the other four states. Once STP has fully converged, all ports on all switches will be in either a forwarding state or a blocking state. All other port states are transitioning states between blocking and forwarding.

When STP is initialized, all ports start in the blocking state to prevent bridge loops. If a switch determines that a blocking port must transition to a forwarding state, the blocked port will first move into a listening state, where it begins sending Bridge Protocol Data Units (BPDUs). Next, the port will transition to a learning state, which allows it to populate its Media Access Control (MAC) address table with addresses learned on the port, but it does not yet forward data frames. Finally, it moves into the forwarding state, where the port is capable of sending and receiving data. The switch only learns MAC addresses during the learning and forwarding states.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Licensed to Berend Post berend.post@it-university.nl

Question 330

You have successfully configured a router, but it prompts you to run Setup mode every time the router is restarted. Based on the following output, what could be causing this problem?

```
RouterA# show version

Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-JS-L), Version
11.3(6), RELEASE SOFTWARE (fc1)

Copyright 1986-1998 by Cisco Systems, Inc.
Compiled Tue 06-Oct-98 22:17 by kpma
Image text-base: 0x03048CF4, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE
SOFTWARE (fc1)

RouterA uptime is 25 minutes
System restarted by power-on
System image file is "flash:c2500-js-l_113-6.bin", booted via flash

Cisco 2500 (68030) processor (revision D) with 4096K/2048K bytes of memory.
Processor board ID 04203139, with hardware revision 00000000
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2142
```

- ☐ The router does not have sufficient flash memory.
- ☒ The configuration register is incorrect.
- ☐ The configuration file could not be found in NVRAM.
- ☐ The router could not locate a configuration file over the network.

Explanation:

Explanation:

The configuration register is incorrect. The configuration register value of 2142 is preventing the router from loading the configuration file from NVRAM.

The router configuration register is used to control various aspects of the router boot sequence, and defaults to a value of 2102. A configuration register of 2102 indicates that the router should boot normally, which consists of loading the Internetwork Operating System (IOS) into RAM, then loading the saved configuration file from Non-Volatile RAM (NVRAM) to configure the router.

Licensed to Berend Post berend.post@it-university.nl

Changing the configuration register to 2142 tells the router to bypass the saved configuration in NVRAM. This causes the router to boot with a default running configuration, and prompt to run the Initial Configuration Dialog (or Setup mode). Changing the configuration register to 2142 is necessary to perform password recovery or to bypass any other aspect of a saved configuration that might be causing problems. After the situation is resolved, the configuration register would then be changed back to the default of 2102 with the following command:

Router(config)# config-register 0x2102

The router is successfully loading the IOS from flash memory, so insufficient flash memory is an incorrect answer.

The configuration register is instructing the router to bypass the configuration file in NVRAM, so it is incorrect to state that the configuration file could not be found in NVRAM.

The configuration register is instructing the router to bypass the configuration file in NVRAM, so it is incorrect to state that the router could not locate a configuration file over the network.

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Cisco > Product Support > Routers > Cisco 10000 Series Routers > Troubleshoot and Alerts > Troubleshooting TechNotes > Use of the Configuration Register on All Cisco Routers > Document ID: 50421

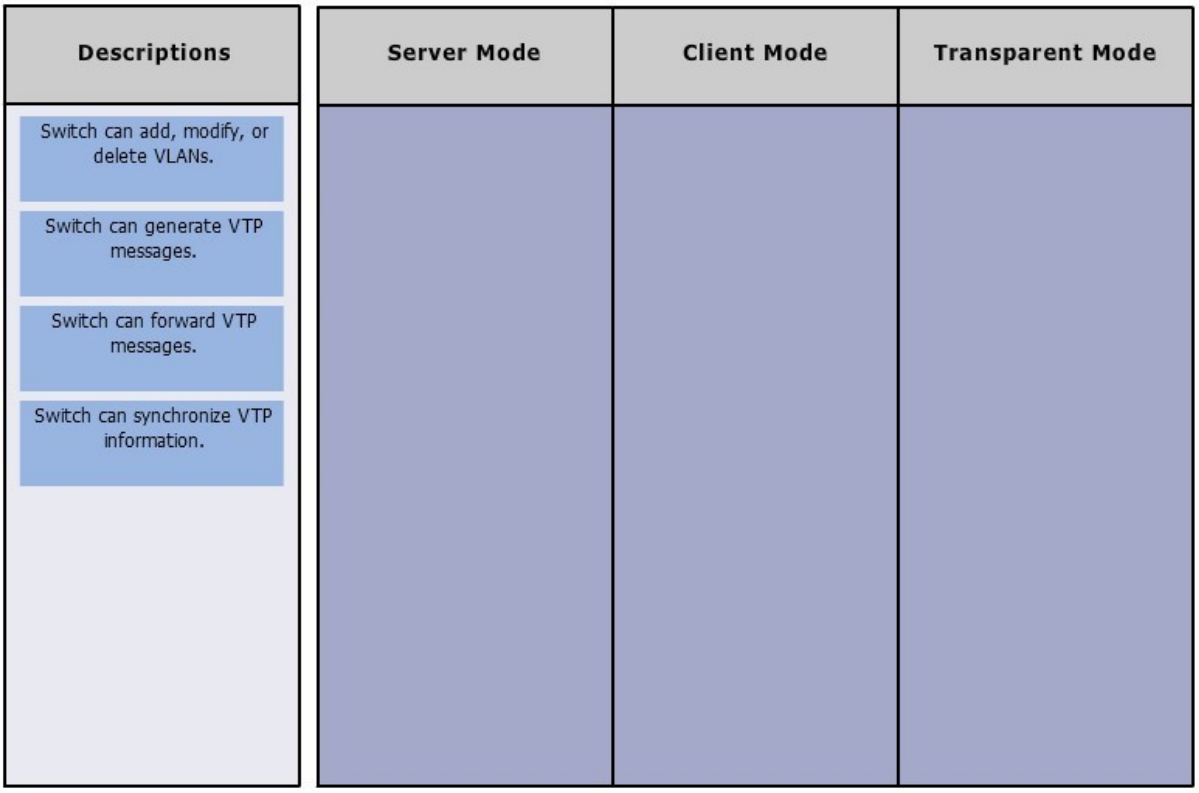
Cisco > Cisco IOS Configuration Fundamentals Command Reference > config-register

Licensed to Berend Post berend.post@it-university.nl

Question 331

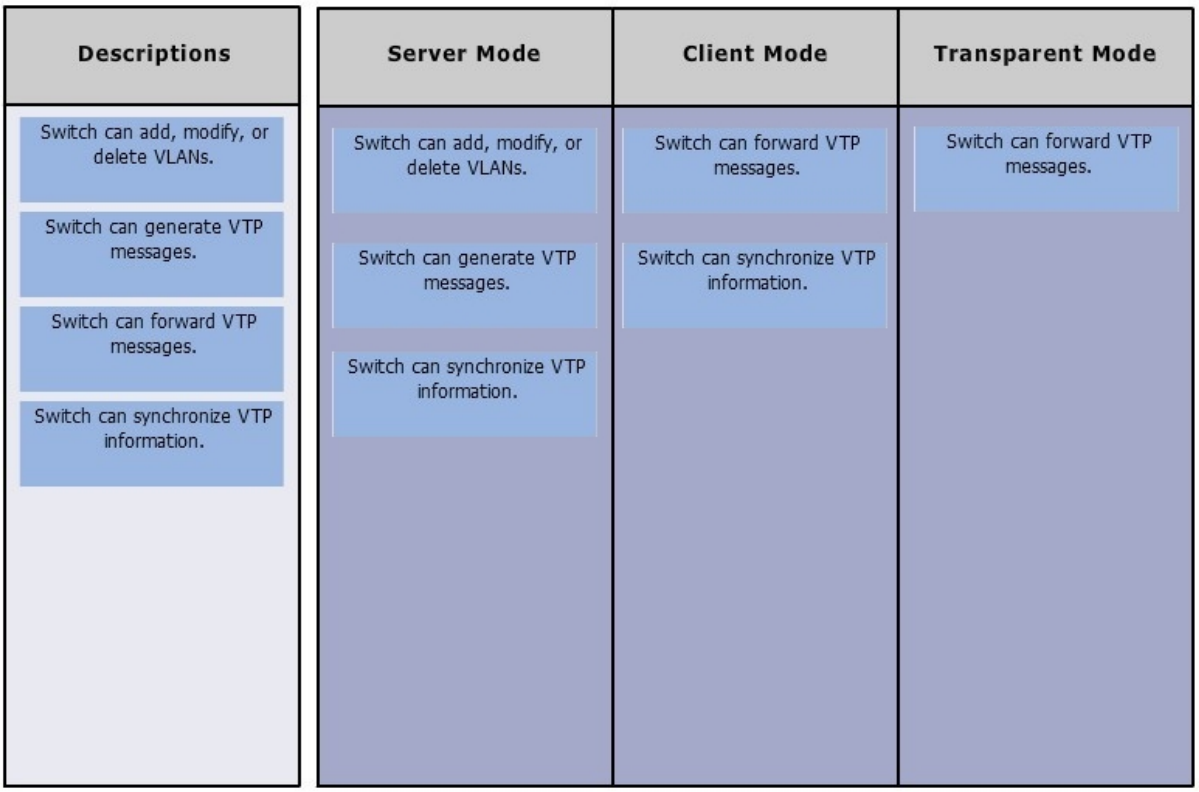
DRAG DROP

Click and drag the VLAN Trunking Protocol (VTP) mode descriptions on the left to their corresponding VTP modes on the right. (The descriptions on the left can be used more than once.)



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

Explanation:

VTP server mode is the default VTP mode.

VTP is a proprietary Cisco protocol used to share VLAN configuration information between Cisco switches on trunk connections. VTP allows switches to share and synchronize their VLAN information, which ensures that your network has a consistent VLAN configuration.

In VTP server mode:

Switch can create, modify, or delete VLANs.

Switches send/forward advertisements.

Switches synchronize VTP information.

VLAN information is saved in Non-Volatile RAM (NVRAM).

In VTP Client mode:

Switches forward advertisements.

Switches synchronize VTP information.

Licensed to Berend Post berend.post@it-university.nl

VLAN information is not saved in NVRAM.

In VTP Transparent mode:

Switch can create, modify, or delete VLANs.

Switches forward advertisements.

Does not synchronize VTP information.

VLAN information is saved in NVRAM.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot inter-VLAN routing

References:

Support > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Configure > Configuration Examples and TechNotes > Configuring VLAN Trunk Protocol (VTP)

CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

Question 332

Which of the following commands would instruct OSPF to advertise ONLY the 192.168.10.0/24 network in Area 0?

- ☒ Router(config)# router ospf 1
- ☒ Router(config-router)# network 192.168.10.0 0.0.0.255 area 0
- ☐ Router(config)# router ospf 1
- ☐ Router(config-router)# network 192.168.11.0 0.0.0.255 area 0
- ☐ Router(config)# router ospf 1
- ☐ Router(config-router)# network 192.168.10.0 255.255.255.0 area 0
- ☐ Router(config)# router ospf 1
- ☐ Router(config-router)# network 192.168.10.0 0.0.255.255 area 0

Explanation:

Explanation:

The command Router(config-router)# network 192.168.10.0 0.0.0.255 area 0 would instruct OSPF to advertise the 192.168.10.0 network in Area 0. It is executed in OSPF process 1 configuration mode, as

Licensed to Berend Post berend.post@it-university.nl

indicated by the prompt Router(config-router)#. This command correctly states the network as 192.168.10.0 and uses the proper wildcard mask of 0.0.0.255.

The command Router(config-router)# network 192.168.11.0 0.0.0.255 area 0 is incorrect because it advertises the 192.168.11.0/24 network instead of the 192.168.10.0/24 network.

The command Router(config-router)# network 192.168.10.0 255.255.255.0 area 0 is incorrect because it uses a regular mask instead of a wildcard mask.

The wildcard mask in OSPF network statements must be expressed inversely, and not as a regular subnet mask. If the network you are configuring for OSPF operation is 192.168.10.0/24, then the inverse version of a /24 mask (or 255.255.255.0) would be 0.0.0.255. The correct command, Router(config-router)# network 192.168.10.0 0.0.0.255 area 0,will configure OSPF to run over any local interfaces assigned an IP address beginning with 192.168.10, since the inverse mask dictates that the first three octets must be a match.

The command Router(config-router)# network 192.168.10.0 0.0.255.255 area 0 is incorrect because it uses an improper wildcard mask. This mask would instruct OSPF to advertise any network with a prefix longer than the 192.168.0.0/16 network.

When routing does not seem to be working correctly, one of the first things to check is whether OSPF is operating on the proper interfaces. OSPF is enabled by network statements. To verify the network statements that were entered, you should execute the show run command and examine the output. If the network statement is configured so that the interface on the router is not in that network, OSPF will not operate on that interface. For example, suppose that Router A has an interface of 192.168.5.1/30 and the show run command produces the following output:

<output omitted>

router ospf 2 area 0

network 192.168.5.0 0.0.0.4

In this case, OSPF will not operate on the interface because the router interface is not in the network indicated by the network statement. The problem is not the network address but the wildcard mask. For a 30-bit mask, the wildcard should be 0.0.0.3, not 0.0.0.4. The wildcard mask can be determined by subtracting the regular mask value in the last octet (252) from 255, which is 3. The solution would to remove the incorrect statement and enter the correct statement as follows:

routerA(config)# router ospf 2 area 0

 Licensed to Berend Post berend.post@it-university.nl

no network 192.168.5.0 0.0.0.4 area 0

network 192.168.5.0 0.0.0.3 area 0

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Cisco > Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T > Part 6: OSPF > Configuring OSPF > OSPF Configuration Task List > Enabling OSPF

Question 333

Which of the following statements are TRUE regarding the following output? (Choose all that apply.)

```
Router# show ip route

Gateway of last resort is 192.168.15.1 to network 0.0.0.0

<<output omitted>>
D 192.168.10.0 [90/2172416] via 192.168.15.254, 0:01:42, Serial0/1/0
C 192.168.14.0 is directly connected, Serial0/0/0
D 192.168.52.0 [90/2172416] via 192.168.15.254, 0:00:35, Serial0/1/0
[90/2172416] via 192.168.15.5, 0:02:05, Serial0/0/0
C 192.168.15.0 is directly connected, Serial0/1/0
C 192.168.20.0 is directly connected, Serial0/0/1
S 192.168.50.0 [1/0] via 192.168.53.1
C 192.168.33.0 is directly connected, Loopback1
D 192.168.25.0 [90/2196545] via 192.168.20.254, 0:01:20, Serial0/0/1
```

- ☐ There are four default routes on this router.
- ☐ There are four physically connected interfaces on this router.
- ☒ This router is running EIGRP.
- ☐ The metric for the routes learned via a routing protocol is 90.
- ☒ A packet for the 192.168.52.0 network will be load-balanced across two paths.

Explanation:

Explanation:

This router is running EIGRP and a packet for the 192.168.52.0 network will be load-balanced across two paths.

Licensed to Berend Post berend.post@it-university.nl

EIGRP routes display with a D code in the leftmost column of the show ip route command. The D stands for Diffusing Update Algorithm (DUAL), which is the algorithm used by EIGRP to determine the best and potential backup paths to each remote network. There are four EIGRP-learned routes in this exhibit.

When two routes with equal metrics exist in the routing table, EIGRP will send packets using both paths. In the output there are two routes listed for the 192.168.52.0 network. Both have the same metric value (2172416). Therefore, packets will be sent to that network via the Serial 0/1/0 interface to the neighbor at 192.168.15.254 and via the Serial 0/0/0 interface to the neighbor at 192.168.15.5. Both paths, either directly or indirectly, lead to the 192.168.52.0 network, and both paths have the same cost.

There are not four default routes on this router. The D represents EIGRP-learned routes, not default routes. There is one default route, as indicated by the line of output that says Gateway of last resort is 192.168.15.1 to network 0.0.0.0. Because Serial0/1/0 is directly connected to the 192.168.15.0 network, packets that are destined for networks not found in the routing table will be sent out on that interface.

The C in the leftmost column of the show ip route command represents directly connected networks, of which there are four in the exhibit. Closer examination, however, reveals that one of these entries (for network 192.168.33.0) is connected to a loopback interface (Loopback1), as opposed to a physical interface:

C 192.168.33.0 is directly connected, Loopback1

Loopback interfaces are virtual, software interfaces that appear in the routing table, but do not represent a physical interface on the router. Therefore, there are three physically connected interfaces on this router, not four.

The metric for the routes learned via a routing protocol is not 90. The 90 in the scenario output is the administrative distance (AD) of the route, and the 2196545 is the metric value (see below):

D 192.168.25.0 [90/2196545] via 192.168.20.254, 0:01:20, Serial0/0/1

Objective:

Routing Fundamentals

Sub-Objective:

 Licensed to Berend Post berend.post@it-university.nl

Interpret the components of routing table

References:

Question 334

Which layer in the Open Systems Interconnection (OSI) model defines an Internet Protocol (IP) address that helps in selecting the route to the destination?

- ☐ Data Link
- ☒ Network
- ☐ Application
- ☐ Transport

Explanation:

Explanation:

The Network layer in the OSI model defines a logical address that helps select the route to the destination. Logical addresses, such as IP addresses or IPX-SPX addresses, are used by routers to forward the packets to the destination. This is accomplished systematically by comparing the destination address with the network addresses listed in the routing table. The logical layout of the network is also defined at this layer. The Network layer is primarily concerned with logical addressing, routing, and path determination.

Protocol data units (PDUs) are called packets at the Network layer. The information that is applied at this layer, which consists of IP addresses, is used in the routing process.

The Data Link layer does not define an IP address. This layer ensures the reliable transmission of data across a network and defines the Media Access Control (MAC) address, which defines the physical device addressing. This layer also defines the format of the header and trailer.

Protocol data units (PDUs) are called frames at the Data Link layer. The information that is applied at this layer, which consists of MAC addresses, is used in the switching process.

The application layer does not define an IP address. The application layer is responsible for interacting directly with the application and provides application services, such as e-mail, FTP, and Telnet. It also defines the user authentication process.

The Transport layer does not define an IP address. 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.

Licensed to Berend Post berend.post@it-university.nl

Protocol data units (PDUs) are called segments at the Transport layer, where the two protocols TCP and UDP operate. Windowing, which is the real-time management of the number of packets that can be received without an acknowledgement, is handled by TCP at this layer.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast OSI and TCP/IP models

References:

Cisco Documentation > Internetworking Technology Handbook > Internetworking Basics>Internet Protocols

Question 335

Which of the following commands helps you determine the Layer 1 and Layer 2 up/down status of a Cisco interface?

- ☐ show controllers
- ☐ show running-config
- ☐ show interfaces trunk
- ☒ show interfaces

Explanation:

Explanation:

The show interfaces command displays the Layer 1 and Layer 2 operational status of an interface, along with other information.

Licensed to Berend Post berend.post@it-university.nl

```
Router# show interfaces
Ethernet 1 is up, line protocol is up
Hardware is MCI Ethernet, address is 0000.0c00.750c (via 0000.0c00.750c)
Internet address is 205.108.28.8, subnet mask is 255.255.0.0
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 10:09*: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, 586 runts, 705 giants
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
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Output queue: 7/64/0 (size/threshold/drops)
                     Conversations 2/9 (active/max active)
```

Of interest in this output is the information contained on line 14 (also shown below). The figures for Runts and Giants (packets that are either too large or too small) indicate that collisions are occurring or that the NIC is malfunctioning:

Received 354125 broadcasts, 586 runts, 705 giants

As a part of troubleshooting this increase in collisions, you can also identify the speed of the interface by reading line 4, which says the bandwidth is 10000 Kbit, indicating a FastEthernet interface.

MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255

You can also specify a particular interface for which information should be displayed, as shown below:

Router# show interfaces ethernet 0/0

Ethernet0/0 is administratively down, line protocol is down

Hardware is AmdP2, address is 0003.e39b.9220 (via 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

 Licensed to Berend Post berend.post@it-university.nl

Keepalive set (10 sec)

ARP type: ARPA, ARP Timeout 04:00:00

<<output omitted>>

The sample output indicates that interface Ethernet 0/0 is in an administratively down, line protocol is down state. The first statement indicates the Layer 1 (Physical) status, while the second statement indicates the Layer 2 (Data Link) status of the interface. A status of administratively down always indicates that the interface is in a shutdown state; the interface can be activated by executing the command no shutdown. This command also indicates the configured bandwidth of the interface (10000 Kbit in this case).

The following lines of information concern the Physical layer:

Hardware is AmdP2, address is 0003.e39b.9220 (via 0003.e39b.9220)

Ethernet0/0 is administratively down, line protocol is down

This output indicates that the link has not been enabled. There are other combinations of up and down states that can indicate other conditions. For example, the following indicates the link is functioning:

Ethernet0/0 is up, line protocol is up

The output below indicates a problem at the other end of the link, perhaps meaning that the interface on the other end has not been enabled or that the port to which it is connected has been disabled.

Ethernet0/0 is up, line protocol is down (not connect)

The following lines of information concern the Data Link layer:

Encapsulation ARPA

line protocol is down

The show controllers command provides Layer 1 information only, including the type of cable detected (DTE/DCE) on a serial interface.

 Licensed to Berend Post berend.post@it-university.nl

The show running-config command displays the current active configuration of the router, but does not indicate the operational status of its interfaces.

The show interfaces trunk command will not show the Layer 1 and Layer 2 up/down status of a Cisco interface. It will show all interfaces configured to be trunks. This command is very useful when you need to locate trunk interfaces on a switch with which you are not familiar. In the output of the command below, the three trunking interfaces are the Fa0/3, Fa0/9, and Fa0/12 interfaces.

```
Switch# show int trunk
Port Mode               Encapsulation          native vlan
Fa0/3               on                  802.1q           1
Fa0/9               desirable            802.1q           1
Fa0/12          desirable           802.1q           1
```

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Cisco > Catalyst 6500 Series Cisco IOS Command Reference, 12.1 E > show bootvar to show ip cache > show interfaces

Licensed to Berend Post berend.post@it-university.nl

Question 336

You have configured a router as shown in the following output:

```
ip dhcp pool POOLNAME
network 10.2.10.0 255.255.255.0
default-router 10.2.10.254
dns-server 10.6.1.200
!
interface fastethernet0/0
ip nat inside
!
interface serial0/1
ip address 200.14.3.25 255.255.255.252
ip nat outside
!
access-list 1 permit 10.2.10.0 0.0.0.255
!
ip nat pool NATPOOL 205.2.1.1 205.2.1.14 netmask 255.255.255.240
ip nat inside source list 1 pool NATPOOL
```

Hosts on the LAN cannot receive an IP address. What is wrong?

- ☐ The IP address on the serial interface is incorrect.
- ☐ The default-router command in the DHCP pool is incorrect.
- ☒ An IP address needs to be configured on the FastEthernet interface.
- ☐ The NAT pool is not large enough.

Explanation:

Explanation:

An IP address needs to be configured on the FastEthernet interface. Dynamic Host Control Protocol (DHCP) is used to dynamically provide IP network configurations to workstations as they are booted up. DHCP minimizes network administration overload, allowing devices to be added to the network with little or no manual configuration.

The router configuration in the scenario has created a DHCP address pool called POOLNAME. The network statement in the exhibit, network 10.2.10.0 255.255.255.0, identifies the range of IP addresses that the pool will provide to host systems (10.2.10.0 /24). However, a DHCP pool can only provide IP addresses over a subnet to which it is directly connected. Because neither of the interfaces in the exhibit has an IP address on the 10.2.10.0 /24 subnet, the solution is to assign the FastEthernet0/0 interface the IP address specified in the default-router statement, 10.2.10.254 /24.

The IP address on the serial interface has no impact on the DHCP pool.

The default-router statement is correctly providing the IP address that DHCP hosts will use as their default gateway. The problem is not with the default-router statement, but with the lack of a correct IP address assigned to the FastEthernet0/0 interface.

Licensed to Berend Post berend.post@it-university.nl

The NAT configuration in the exhibit has no impact on the DHCP pool. If the NAT pool were not large enough, the result would be that some of the hosts would be able to get to the Internet and others would not. For example, the output from the diagram shown below indicates that there are fourteen addresses in the pool (205.2.1.1 to 205.2.1.14). If the network contained 30 computers, only fourteen would be able to use the Internet at the same time because of the number of public addresses in the pool:

ip nat pool NATPOOL 205.2.1.1 205.2.1.14 netmask 255.255.255.240

ip nat inside source list 1 pool NATPOOL

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify DHCP on a router (excluding static reservations)

References:

Cisco > Support > Cisco IOS Software > Configuring the Cisco IOS DHCP Server > Configuring DHCP Address Pools

Question 337

Which Cisco Internetwork Operating System (IOS) command will you use to view the details of each interface on a router?

- ☐ show controllers
- ☐ show interfaces ethernet
- ☒ show ip interface brief
- ☐ show interfaces loopback

Explanation:

Explanation:

The show ip interface brief command is used to view the details of each interface on a router. The output of the command displays the interfaces, the IP addresses configured on each interface, the method, the status, and the protocol.

The following is a sample output of this command:

Interface IP-Address OK? Method Status Protocol

 Licensed to Berend Post berend.post@it-university.nl

Ethernet0 10.105.00.5 YES NVRAM up up

Ethernet1 unassigned YES unset administratively down down

Loopback0 10.105.200.5 YES NVRAM up up

Serial0 10.105.100.5 YES NVRAM up up

Serial1 10.105.40.5 YES NVRAM up up

Serial2 10.105.100.5 YES manual up up

Serial3 unassigned YES unset administratively down down

The show controllers command is incorrect. The show controllers command is used to view hardware-related information on router and switch interfaces. It is useful for troubleshooting and diagnosing issues with interfaces. One of the many useful pieces of information yielded by command is the type of cable connected to the interface. When you are using a V.35 cable to connect two serial interfaces directly between two routers, one of the routers must be configured to provide the clocking on the line and it must be the router with the DCE end of the cable. You can determine which router has that end by executing this command, which would display output similar to the following:

R2#show controllers serial 0

HD unit 0, idb = 0xDFE73, driver structure at 0xE52FF

Buffer size 1524 HD unit 0, V.35 DCE cable, clockrate 64000

In the above example, the DCE end of the V.35 cable is connected to this router. Therefore, this is the router that must be configured with a clockrate. The output demonstrates that this requirement was already met.

The show interfaces ethernet command is incorrect because this command will display information only for Ethernet interfaces.

The show interfaces loopback command is incorrect because this command will show information regarding loopback interfaces only.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Cisco IOS IP Addressing Command Reference > show ip interface brief

Question 338

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.)

- ☒ Router 10 has not yet been configured for authentication
- ☐ Router 10 is configured for RIPv2 and Router 8 is configured for RIP v1.
- ☐ There is a connectivity problem between the routers.
- ☐ Router 10 is over 16 hops away
- ☒ The password is not correct.

Explanation:

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:

 Licensed to Berend Post berend.post@it-university.nl

*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:

Cisco IOS Debug Command Reference, Release 12.4 > Commands: debug ip http all through debug ip rsvp > debug ip rip

Question 339

Which of the following methods of tunneling Internet Protocol version 6 (IPv6) traffic through an IPv4 network increases protocol overhead because of IPv6 headers?

- ☐ Protocol translation
- ☐ IPv6 over dedicated WAN links
- ☐ Dual-Stack Backbones
- ☒ IPv6 over IPv4 tunnels

Explanation:

Explanation:

IPv6 over IPv4 tunnels is a method of tunneling IPv6 traffic through an IPv4 network that eliminates the need to create separate circuits to connect to the IPv6 networks. This model increases protocol overhead because of IPv6 headers.

The following deployment models are available for IPv4 to IPv6 migration:

IPv6 over IPv4 tunnels: IPv6 traffic is encapsulated into IPv4 packets. Then these packets are transferred over IPv4 WAN. This model eliminates the need to create separate circuits to connect to the IPv6 networks. This model increases protocol overhead because of the IPv6 headers and requires both ends to be capable of both protocols.

Protocol translation: A method allowing an IPv6 host to communicate with an IPv4 host. This is accomplished with the help of Network Address Translation - Protocol Translation (NAT-PT) used to configure translation between IPv6 and IPv4 hosts. NAT-PT allows communication between IPv6 hosts and applications, and native IPv4 hosts and applications.

 Licensed to Berend Post berend.post@it-university.nl

IPv6 over dedicated WAN links: A new deployment of IPv6 is created. In this model, IPv6 hierarchy, addressing, and protocols are used by all nodes. However, this model involves cost for creating IPv6 WAN circuits. This solution is not designed for LAN translation but rather translation over WAN links.

Dual-Stack Backbones: A hybrid model in which backbone routers have dual-stack functionality, which enables them to route both IPv4 and IPv6 packets. It is suitable for an enterprise that uses both IPv4 and IPv6 applications. Running IPv6 and IPv4 together in a network is known as dual-stack routing.

Objective:

Network Fundamentals

Sub-Objective:

Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

References:

Cisco > Technology Support > IP > IPv6 > Configure > Configuration Examples and TechNotes > Tunneling IPv6 through an IPv4 Network > Document ID: 25156

Question 340

Which of the following items are NOT required to match for two routers to form an OSPF adjacency?

- ☐ Area IDs
- ☐ Hello/Dead timers
- ☐ Passwords (if OSPF authentication has been configured)
- ☒ Process IDs

Explanation:

Explanation:

All of the listed items must match except for the process IDs. The process IDs are locally significant, which keeps multiple instances of OSPF separate on a router, and do not need to match between neighboring routers for the adjacency to form. Process identifiers can be valued from 1 to 65535.

Adjacencies must be formed before routing updates can be exchanged. OSPF routers will form neighbor adjacencies on common subnets if the following three items match:

Area IDs

Hello/Dead timers

Passwords (if OSPF authentication has been configured)

Licensed to Berend Post berend.post@it-university.nl

Once an adjacency has been formed it will be maintained by the exchange of Hello messages. On a broadcast medium like Ethernet, they will be sent every 10 seconds. On point-to-point links, they will be sent every 30 seconds.

The show ip ospf interface interface number command can be used to display the state of the DR/BDR election process.

Consider the following output:

```
RouterA# show ip ospf interface fastethernet0/0

Fastethernet0/0 is up, line protocol is up
Internet Address 192.168.30.2/24, Area 0
Process ID 1, Router ID 192.168.45.1, Network Type BROADCAST,
Cost: 10
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.45.1, Interface address
192.168.30.2
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 00:00:06

RouterB# show ip ospf interface fastethernet0/0
Fastethernet0/0 is up, line protocol is up
Internet Address 192.168.30.1/24, Area 0
Process ID 2, Router ID 192.168.60.1, Network Type BROADCAST,
Cost: 10
Transmit Delay is 1 sec, State DR, Priority 2
Designated Router (ID) 192.168.60.1, Interface address
192.168.30.1
No backup designated router on this network
Timer intervals configured, Hello 30, Dead 60, Wait 40,
Retransmit 5
Hello due in 00:00:12
```

The timer intervals' configured output reveals that RouterA is showing a Hello timer of 10 seconds and a Dead timer of 40 seconds. RouterB has a Hello timer of 30 seconds and a Dead timer of 60 seconds. Hello/Dead timers have to match before OSPF routers will form an adjacency. If you executed the debug ip ospf events command on one of the routers, the router at serial /01 will not form a neighbor relationship because of mismatched hello parameters:

RouterA# debug ip ospf events

OSPF events debugging is on

 Licensed to Berend Post berend.post@it-university.nl

RouterA#

*Nov 9 05:41:21.456:OSPF:Rcv hello from 10.16.2.3 area 0 from Serial0/1

192.168.35.1

*Nov 9 05:41:21.698:OSPF:Mismatched hello parameters from

192.168.35.1

Hellos are used to establish neighbor adjacencies with other routers. On a point-to-point network, hello packets are sent to the multicast address 224.0.0.5, which is also known as the ALLSPFRouters address.

Area IDs have to match for OSPF routers to form an adjacency. Both of these routers have the interface correctly configured in matching Area 0.

The interface priorities do not have to match for OSPF routers to form an adjacency. Interface priorities can be configured to control which OSPF router becomes the designated router (DR) or backup designated router (BDR) on a multi-access network segment.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

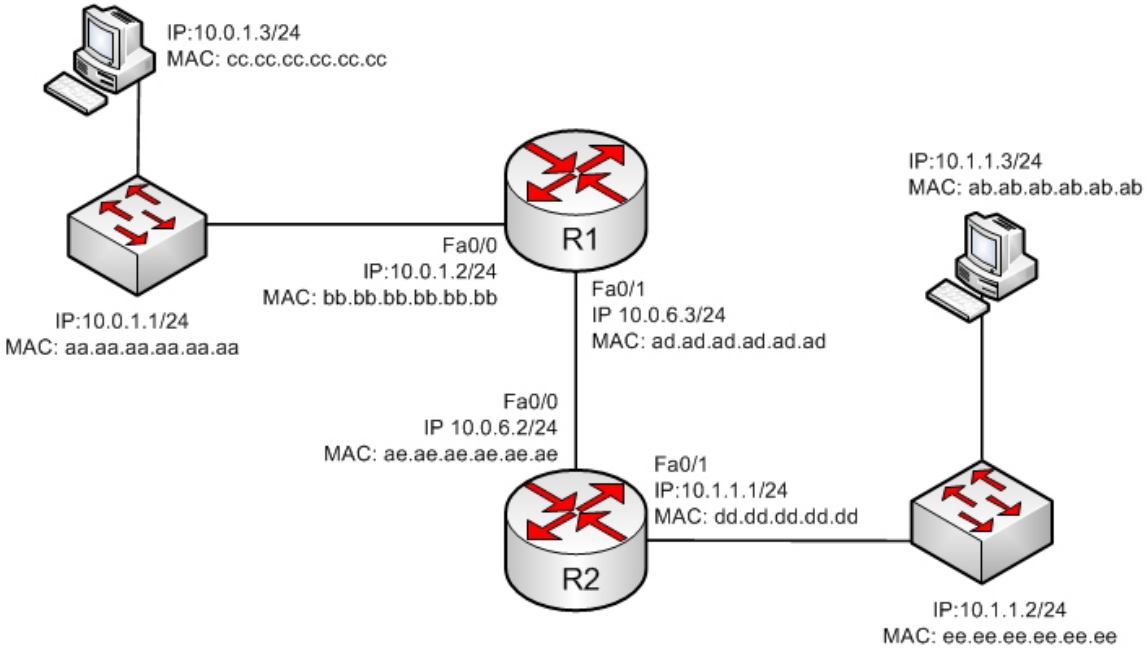
References:

Cisco > Home > Support > Technology Support > IP > IP Routing > Design > Design TechNotes > OSPF Neighbor Problems Explained

Licensed to Berend Post berend.post@it-university.nl

Question 341

In the diagram below, when a packet sent from the PC at 10.0.1.3 to the PC at 10.1.1.3 leaves the Fa0/1 interface of R1, what will be the source and destination IP and MAC addresses?



- ☐ source IP 10.1.1.2 destination IP 10.1.1.3
- ☐ Source MAC ad.ad.ad.ad.ad.ad destination MAC ab.ab.ab.ab.ab.ab
- ☐ source IP 10.1.1.1 destination IP 10.1.1.3
- ☐ Source MAC ad.dd.dd.dd.dd.dd.dd destination MAC ab.ab.ab.ab.ab.ab
- ☒ source IP 10.0.1.3 destination IP 10.1.1.3
- ☒ Source MAC ad.ad.ad.ad.ad.ad destination MAC ae.ae.ae.ae.ae.ae
- ☐ source IP 10.0.6.3 destination IP 10.1.1.3
- ☐ Source MAC ad.ad.ad.ad.ad.ad destination MAC ae.ae.ae.ae.ae.ae

Explanation:

Explanation:

The source IP address will be 10.0.1.3 and the destination IP address will be 10.1.1.3. The source MAC address will be ad.ad.ad.ad.ad.ad and the destination MAC address will be ae.ae.ae.ae.ae.ae.

The source and destination IP addresses never change as the packet is routed across the network. The MAC address will change each time a router sends the packet to the next router or to the ultimate destination. The switches do not change either set of addresses in the header; they just switch the frame to the correct switch port according to the MAC address table. Therefore, when the packet leaves R1, the source MAC address will be that of R1 and the destination MAC address will be that of the Fa0/0 interface of R2. The IP addresses will be those of the two workstations, 10.0.1.3 and 10.1.1.3.

Licensed to Berend Post berend.post@it-university.nl

When the workstation at 10.0.1.3 starts the process, it will first determine that the destination address is in another subnet and will send to its default gateway (10.0.1.2). It will perform an ARP broadcast for the MAC address that goes with 10.0.1.2, and R1 will respond with its MAC address, bb.bb.bb.bb.bb.bb.

After R2 determines the next-hop address to send to 10.0.1.3 by parsing the routing table, it will send the packet to R1 at 10.0.6.2. When R2 receives the packet, R2 will determine that the network 10.0.1.0/24 is directly connected and will perform an ARP broadcast for the MAC address that goes with 10.0.1.3. The workstation at 10.0.1.3 will respond with its MAC address, ab.ab.ab.ab.ab.ab.

Objective:

Routing Fundamentals

Sub-Objective:

Describe the routing concepts

References:

Cisco > IOS Technology Handbook > Routing Basics

Question 342

Which of the following statements is true with regard to SDN?

- ☐ It combines the control plane and the data plane
- ☐ It separates the data plane and the forwarding plan
- ☒ It implements the control plane as software
- ☐ It implements the data plane as software

Explanation:

Explanation:

In Software-defined networking (SDN), the control plane is separated from the data (or forwarding) plane and is implemented through software. The data plane remains on each physical device but the control plane is managed centrally for all devices though software.

SDN does not combine the data and control plane. Instead it decouples them.

SDN does not separate the data plane and the forwarding plan. These are both names for the same plane; that is, a data plane is a forwarding plane.

Licensed to Berend Post berend.post@it-university.nl

SDN does not implement the data plane as software. The data plane remains on each physical device.

Objective:

Infrastructure Management

Sub-Objective:

Describe network programmability in enterprise network architecture

References:

Software Defined Networking: The Cisco approach

Question 343

Which protocol is used in redundant network topologies to avoid receiving multiple copies of the same frame?

- ☐ 802.1q
- ☒ Spanning Tree Protocol
- ☐ Cisco Discovery Protocol
- ☐ Routing Information Protocol

Explanation:

Explanation:

Spanning Tree Protocol (STP) is used to remove switching loops in redundantly configured switched environments, and to create a single active Layer 2 path between any two network segments. This eliminates the chance of multiple copies of the same unicast frame being sent in the LAN. It also prevents broadcast packets from creating a broadcast storm when redundant connections exist between the switches. The benefits of STP include:

Prevention of broadcast storms

Prevention of multiple frame copies

Media Access Control (MAC) address database stability

Whenever a network segment can be handled by more than one switch, STP will elect one switch to take responsibility, and the other switches will be placed into a blocking state for the ports connected to that segment. In this way, only one switch receives and forwards data for this segment, which removes the potential for multiple copies of the same frame being generated. For STP to provide this functionality it must be running on all of the switches. Therefore, a properly implemented redundant topology STP is required in order to prevent multiple copies of the same unicast frame from being transmitted.

 Licensed to Berend Post berend.post@it-university.nl

802.1q is a frame tagging method for identifying Virtual LAN (VLAN) memberships over trunk links. Frame tagging ensures identification of individual VLAN frames over a trunk link carrying frames for multiple VLANs. This frame tagging method is a standardized protocol that was developed by The Institute of Electrical and Electronics Engineers (IEEE). Cisco has also developed a proprietary frame tagging method known as Inter-Switch Link (ISL). 802.1q does not mitigate loops or the reception of multiple copies of frames. The IEEE specification for STP is 802.1d.

Cisco Discovery Protocol is a Cisco proprietary protocol used to collect hardware and protocol information for directly connected Cisco devices. CDP has nothing to do with redundant network topologies.

Routing Information Protocol (RIP) is a distance vector routing protocol. It populates routing tables dynamically about the topology changes. However, RIP does not control the receipt of multiple copies of frames in redundant network topologies.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

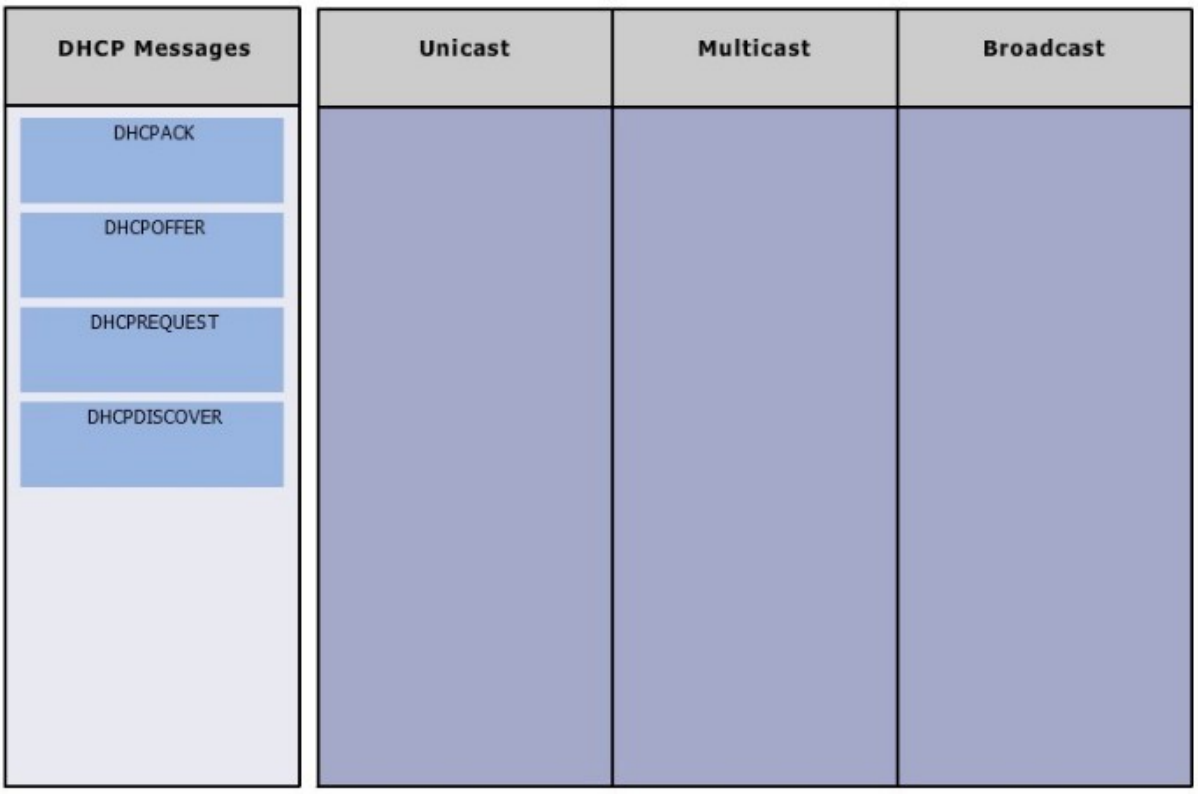
Cisco > Support > Configuring Spanning Tree-Protocol > How STP Works

Licensed to Berend Post berend.post@it-university.nl

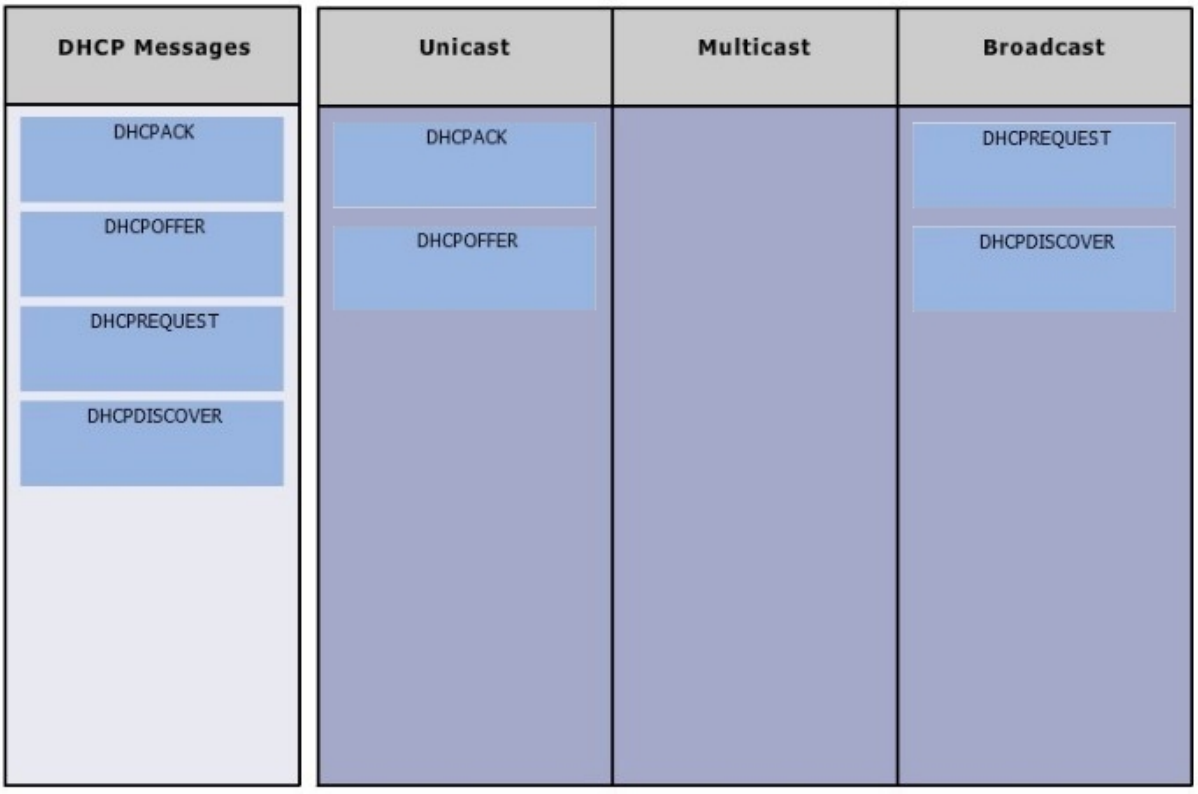
Question 344

DRAG DROP

Group the special DHCP messages exchanged over the network, on the left, into the different transmission types, on the right.



Solution:



Licensed to Berend Post berend.post@it-university.nl

Explanation:

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 Cisco IOS DHCP server:

The client device broadcasts a DHCPDISCOVER broadcast message to locate a Cisco IOS DHCP server.

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.

The client sends back a DHCPREQUEST broadcast, which is a formal request for the offered IP address to the Cisco IOS DHCP server.

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:

Cisco Documentation > Cisco IOS IP Configuration Guide, Release 12.2 > Part 1: IP Addressing and Services > Configuring DHCP

Licensed to Berend Post berend.post@it-university.nl

Question 345

What will be the effects of executing the following set of commands? (Choose all that apply.)

router(config)# router eigrp 44
router (config-router)# network 10.0.0.0
router (config-router)# network 192.168.5.0

- ☒ EIGRP will be enabled in AS 44
- ☐ EIGRP instance number 44 will be enabled
- ☒ EIGRP will be activated on the router interface 10.0.0.2/8
- ☒ EIGRP will be activated on the router interface 192.168.5.9/24
- ☒ EIGRP will be activated on the router interface 10.0.5.8/16
- ☐ EIGRP will be activated on the router interface 192.168.6.1/24

Explanation:

Explanation:

The effects of executing this set of commands will be that Enhanced Interior Gateway Routing Protocol (EIGRP) will be enabled in Autonomous System (AS) 44 and will be active on the router interfaces 10.0.0.2/8,192.168.5.9/24, and 10.0.5.8/16.

The router eigrp 10 command is used to enable EIGRP on a router. The network 10.0.0.0 and network 192.168.5.0 commands are used to activate EIGRP over any interfaces that fall within the major networks 10.0.0.0 and 192.168.5.0, or within any subnets of these classful networks. The network commands in EIGRP configuration ignore any subnet-specific information by default. Since the IP address 10.0.5.8.9/24 is in a subnet of the Class A IP network 10.0.0.0, and only the first octet (byte) of a Class A IP address represents the major (classful) network, the remaining bytes are ignored by the network command.

EIGRP instance number 44 will not be enabled. The number 44 in the command does not represent an instance of EIGRP; it represents an autonomous system (AS) number. The autonomous-system parameter of the router eigrp command (router eigrp 44) specifies the autonomous system number. To ensure that all the routers in a network can communicate with each other, you should specify the same autonomous system number on all routers.

EIGRP will not be activated on the router interface 192.168.6.1/24. This interface does not exist within the Class C network 192.198.5.0 or Class A network 10.0.0.0, or within any of their subnets.

Objective:

Routing Fundamentals

Sub-Objective:

 Licensed to Berend Post berend.post@it-university.nl

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Support > Cisco IOS Software > Configuring EIGRP > Enabling EIGRP

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 10: EIGRP, pp. 389-390.

Question 346

A new security policy has been adopted by your company. One of its requirements is that only one host is permitted to attach dynamically to each switch port. The security settings on all of the ports have been altered from the default settings.

You execute the following command on all switch ports of Switch A:

SwitchA(config-if)# switchport port-security maximum 1

After executing the command, you discover that users in the Sales department are still successfully plugging a hub into a port and then plugging two or three laptops into the hub.

What did you do wrong?

- ☐ The command should be executed at the global prompt.
- ☐ The command should be executed as switchport port-security maximum 0.
- ☐ You also need to execute the switchport port-security violation shutdown command at the global prompt.
- ☒ You also need to execute the switchport port-security violation shutdown command on each switch port.

Explanation:

Explanation:

When configuring switch port security to enforce the policy described in the scenario, two commands are required. One command specifies how many addresses are allowed per switch port and the other tells the switch what to do when a violation occurs. Configuring the first without the second is like creating a rule without enforcing the rule. Both commands must be executed on each switch port, as shown in the following example:

switchA(config)# interface fa0/22

switchA(config-if)# switchport port-security maximum 1

switchA(config-if)# switchport port-security violation shutdown

Licensed to Berend Post berend.post@it-university.nl

By default, ports are configured to shut down on a violation, but the scenario states the default settings have been altered.

The switchport port-security violation command can be set to shutdown, restrict, or protect. The shutdown option shuts down the port if there is a security violation, but does not send an SNMP trap logging the violation. The restrict option drops all packets from insecure hosts at the port-security process level and increments the security-violation count, and can send an SNMP trap. The protect option drops all the packets from the insecure hosts at the port-security process level, but does not increment the security-violation count or send an SNMP trap.

You should not execute either the switchport port-security violation command or the switchport port-security maximum command at the global prompt. Both commands must be executed on each switch port.

You should not execute the command switchport port-security maximum 0. This would tell the switch to not allow any addresses at all per switch port.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport port-security maximum

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport port-security violation

Question 347

Which command would be used to establish static translation between an inside local address and an inside global address?

- ☒ Router(config)# ip nat inside source static local-ip global-ip
- ☐ Router(config)# ip source nat inside static local-ip global-ip
- ☐ Router(config)# ip nat inside static source local-ip global-ip
- ☐ Router(config)# ip nat static inside source local-ip global-ip

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

You should use the following command:

Router(config)# ip nat inside source static local-ip global-ip

You can translate your own IP addresses into globally unique IP addresses when communicating outside of your network. You can configure static or dynamic inside source translation.

To establish static translation between an inside local address and an inside global address, you should use the ip nat inside source static local-ip global-ip command. This static configuration can be removed by entering the no ip nat inside source static global command.

The other options are incorrect as they are not valid Cisco IOS configuration commands.

Objective:

Infrastructure Services

Sub-Objective:

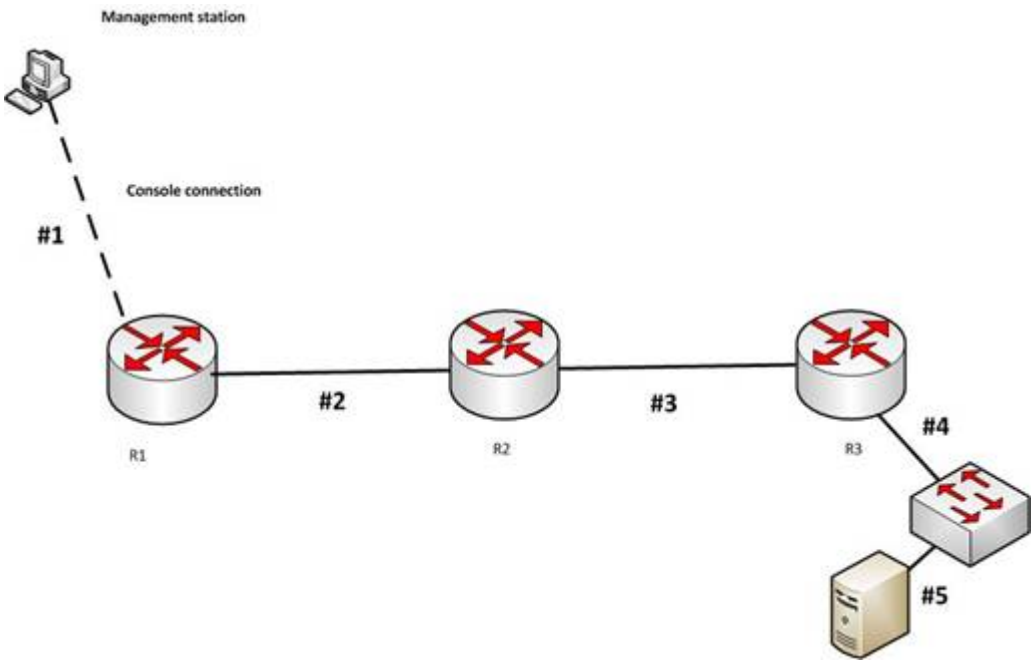
Configure, verify, and troubleshoot inside source NAT

References:

Licensed to Berend Post berend.post@it-university.nl

Question 348

You need to cable the network shown below.



Which of the following is the correct cable for each numbered link?

- ☐ 1-crossover, 2-staight-through, 3-rollover, 4- crossover, 5-crossover
- ☐ 1-straight-through, 2-staight-through, 3-rollover, 4- crossover, 5-crossover
- ☐ 1-crossover, 2-crossover, 3-rollover, 4- crossover, 5-crossover
- ☒ 1-rollover, 2-crossover, 3-crossover, 4- straight-through, 5-straight through

Explanation:

Explanation:

The correct cabling pattern is 1-rollover, 2-crossover, 3-crossover, 4- straight-through, 5-straight through. When selecting cables, the following rules apply:

Router to router- crossover

Router to switch- straight- through

Management station (PC) to router for console session- rolled cable

Switch to switch - crossover

PC to switch- straight through

Objective:

Network Fundamentals

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Select the appropriate cabling type based on implementation requirements

References:

Cisco > Product Support > End-of-Sale and End-of-Life Products > Cisco 7000 Series Routers > Troubleshooting TechNotes > Cabling Guide for Console and AUX Ports > Document ID: 12223

Question 349

Which switch will be selected as the root bridge by Spanning Tree Protocol (STP)?

- ☒ switch with lowest bridge ID
- ☐ switch with lowest IP address
- ☐ switch with lowest Media Access Control (MAC) address
- ☐ switch with lowest number of root ports

Explanation:

Explanation:

STP will use elections to arrive at a fully converged state that will ensure a switching loop free network. It will select:

The root bridge

The root port on each non-root bridge

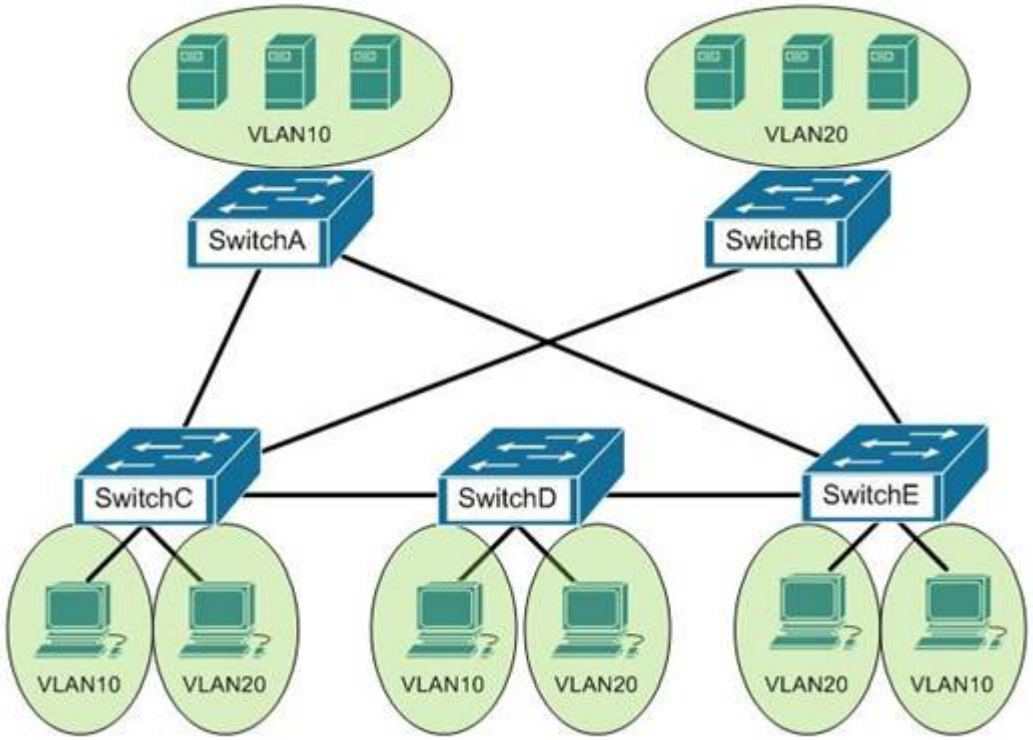
Designated ports on any shared segments with no direct connection to the root bridge.

The switch with the lowest bridge ID will be selected as the root bridge by STP. A bridge ID has two components: the priority number and the MAC address. On Cisco devices, the priority number may range from 0 to 65535. The priority number constitutes the most significant bits of the bridge ID. If you want to ensure that a particular switch in a topology always becomes a root bridge, regardless of the MAC address, you can set the priority number of that switch to the lowest value among all switches in the topology.

Since the selection of the root bridge influences all other decisions and thus the single loop free path for each VLAN, the selection and location of the root bridge is important and best not left to chance. Once you have determined the best switch for the role of root bridge, you can ensure its election by lowering its bridge priority.

It is best for the root bridge to be centrally located with respect to the clients and the servers that generate the most traffic on the VLAN. For example, in the diagram below, if most of the traffic travels between the clients and the servers on VLAN 20, the best choice for the root bridge for VLAN 20 would be SwitchD. SwitchD is centrally located between the clients on VLAN 20 and the servers on VLAN 20.

 Licensed to Berend Post berend.post@it-university.nl



To illustrate the type of inefficient traffic that could occur when care is not given to the location of the root bridge, consider the diagram above and assume that Switch B was chosen the root bridge. Next, assume that traffic needs to go from VLAN 10 connected to Switch C to VLAN 10 connected to Switch A. The shortest path would be from Switch C to Switch A. However, because the only port that is forwarding on Switch C is the port that leads to the root bridge (Switch B), then the actual path would be from Switch C, to Switch B, to Switch E, and then to Switch A.

By default, the priority number of all Cisco switches is configured to a value of 32768. For example, consider three switches in network topology with the following MAC addresses and the same default priority number:

0000.0B02.AAAA

0000.0B02.BBBB

0000.0B02.CCCC

The switch with the lowest MAC address, 0000.0B02.AAAA, will become the root bridge.

The switch with the lowest IP address will not be selected as the root bridge by STP because the IP address of the switch does not influence the selection of the root bridge.

Licensed to Berend Post berend.post@it-university.nl

The switch with the lowest MAC address will not be selected as the root bridge by STP. A combination of priority number and MAC address determines the selection of the root bridge. The MAC address will determine the root bridge only if there is a tie for the switch with the lowest priority number.

The switch with the lowest number of root ports will not be selected as the root bridge by STP. Root ports are the interfaces on non-root bridges. On a non-root bridge, the least-root-cost interface is known as a root port. Therefore, the switch having the fewest root ports is not the root bridge.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Support > Configuring Spanning Tree Protocol > How STP Works > How a Switch or Port Becomes the Root Switch or Port

Cisco Documentation > Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX > Configuring STP and IEEE 802.1s MST > Understanding the Bridge ID

Question 350

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?

- ☒ router(config)#ip nat inside source static 192.168.144.25 202.56.63.102
- ☐ router(config)#ip source nat inside static local-ip 192.168.144.25 global-ip 202.56.63.102
- ☐ router(config)#ip nat static inside source 192.168.144.25 202.56.63.102
- ☐ router(config)#ip nat inside static source 192.168.144.25 202.56.63.102

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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:

Licensed to Berend Post berend.post@it-university.nl

Question 351

```
Routing Protocol is "igrp 120"
Sending updates every 90 seconds, next due in 44 seconds
Invalid after 270 seconds, hold down 280, flushed after 630
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
IGRP maximum hopcount 100
IGRP maximum metric variance 1
Redistributing: igrp 109
Routing for Networks:
172.160.74.0
Routing Information Sources:
Gateway Distance Last Update
172.160.74.18 100 0:56:41
172.160.74.19 100 6d19
172.160.74.22 100 0:25:41
172.160.74.20 100 0:01:04
172.160.74.30 100 0:02:29
Distance: (default is 100)
Routing Protocol is "bgp 18"
Sending updates every 60 seconds, next due in 0 seconds
Outgoing update filter list for all interfaces is 1
Incoming update filter list for all interfaces is not set
Redistributing: igrp 109
IGP synchronization is disabled
Automatic route summarization is enabled
Neighbor(s):
Address FiltIn FiltOut DistIn DistOut Weight RouteMap
192.109.211.17 1
192.109.213.89 1
198.6.255.13 1
172.161.72.18 1
172.161.72.19
172.161.84.17 1
Routing for Networks:
192.108.209.0
192.108.211.0
198.6.254.0
Routing Information Sources:
Gateway Distance Last Update
172.161.72.19 20 0:05:28
Distance: external 20 internal 200 local 200
```

What command produced the preceding output?

- ☐ show ip process
- ☐ show ip route
- ☒ show ip protocols
- ☐ show ip routing process

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The show ip protocols command is used to view the current state of active routing protocols. This command is issued from Privileged EXEC mode. It has the following syntax:

Router# show ip protocols

This command does not have any parameters.

The output was not produced by the command show ip process or the show ip routing process. The show ip routing process and show ip process commands are incorrect because these are not valid Cisco IOS commands.

The output was not produced by the command show ip route. The show ip route command is is used to view the current state of the routing table. An example of the output is shown below.

```
router>show ip route
Codes: C - connected O - OSPF i - IS-IS
S - static IA - inter area L1 - level-1
B - BGP E1 - external type 1 L2 - level-2
E2 - external type 2
* - candidate default
m - route's metric
w - route's weight
S 0.0.0.0/0 directly connected to null 0
C 6.1.1.64/28 directly connected to ethernet 1
C 6.1.1.80/28 directly connected to ethernet 2
C 6.1.1.96/28 directly connected to ethernet 3
C 6.1.1.112/28 directly connected to ethernet 4
S 11.1.0.0/16 via 10.5.0.1 [w:0 m:0]
C 11.5.0.0/16 directly connected to ethernet 0
S 127.0.0.0/8 directly connected to null 0
```

Objective:

Licensed to Berend Post berend.post@it-university.nl

Routing Fundamentals

Sub-Objective:

Interpret the components of routing table

References:

Cisco > Support > Cisco IOS IP Routing: Protocol-Independent Command Reference > show ip protocols

Question 352

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?

- ☐ Disable VTP pruning.
- ☐ Convert all switch ports into trunk ports.
- ☐ Create an access list with permit statements.
- ☒ Install a routing device or enable Layer 3 routing on a switch.

Explanation:

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 of the 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>>

 Licensed to Berend Post berend.post@it-university.nl

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 unnecessary broadcast 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:

Question 353

How many IP addresses are available for hosts in the 192.168.16.64 /26 subnet?

- ☐ 14
- ☐ 30
- ☒ 62
- ☐ 126

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

There are 62 IP addresses available for hosts in the 192.168.16.64 /26 subnet.

The number of host addresses is calculated as 2n - 2, where n is the number of host bits and 2 is subtracted to exclude the network address and the broadcast address.

An IP address has 32 available bits divided into four octets. In the 192.168.16.66 /26 address, the /26 indicates that there are 26 masking bits, or that 26 bits are reserved for the network portion of the address. This leaves 6 bits for the host addresses (32 - 26 = 6).

The following formula is used to calculate the number of IP addresses available for hosts:

Network address: 192.168.16.0

Subnet mask in decimal: 255.255.255.192

Subnet mask in binary: 11111111.11111111.1111111.11000000

Number of bits used for masking = 26

Number of hosts bits in the address = 6

Using the formula for calculating the number of hosts per subnet, we find:

Hosts formula: 2number-of-host-bits - 2

Hosts: 26 - 2 = 62

For subnet 192.168.16.64, the valid host range starts from 192.168.16.65 and runs to 192.168.16.126. For subnet 192.168.16.128, the valid host range starts from 192.168.16.129 and runs to 192.168.16.190.

The options 14, 30, and 126 are incorrect because 62 IP addresses are available for hosts in the 192.168.16.64/26 subnet.

The correct mask for the size network desired is critical to proper network function. For example, assume a router has an interface Fa0/0 hosting a LAN with 20 computers configured as shown in the following output of show interfaces command:

Router# show interfaces

Licensed to Berend Post berend.post@it-university.nl

Fastethernet0 is up, line protocol is up

Hardware address is 000b.12bb.4587

Internet address 192.168.10.30/30

In this example, the computers will not be able to access anything beyond the LAN because the mask /30 only allows for 2 addresses when 21 (including the router interface) are required.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

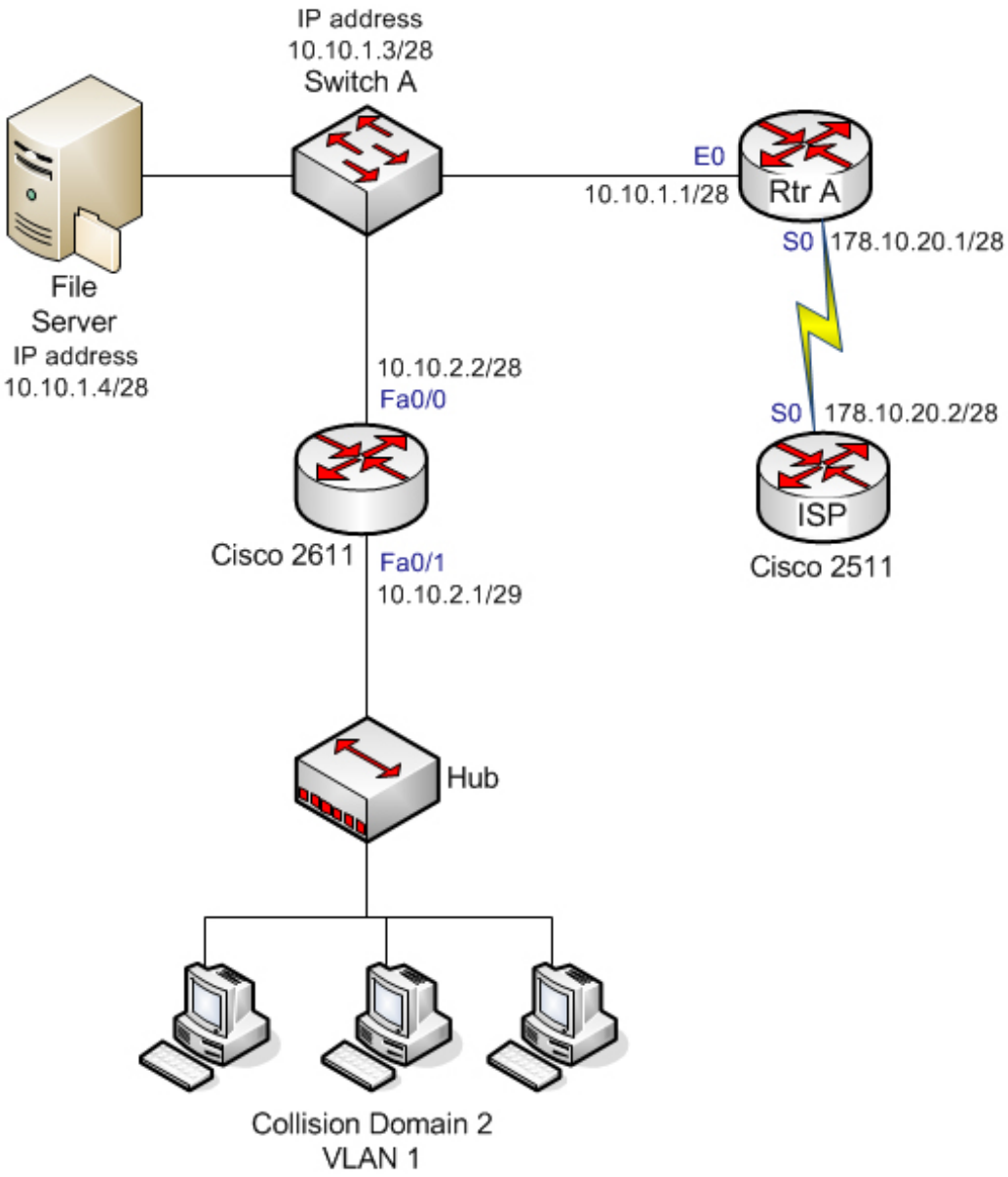
References:

Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Licensed to Berend Post berend.post@it-university.nl

Question 354

What will be the output of the show cdp neighbors detail command issued on Router A? (Click the Exhibit(s) button to view the network diagram.)



- ☐ Device ID: RTR2511
- ☐ Entry address(es):
- ☐ IP address: 178.10.20.1
- ☐ Platform: cisco 2511, Capabilities: Router
- ☐ Interface Serial 0
- ☐ ----------
- ☐ Device ID: RTR2611-Edge
- ☐ Entry address(es):
- ☐ IP address: 10.10.1.2
- ☐ Platform: cisco 2611, Capabilities: Router

Licensed to Berend Post berend.post@it-university.nl

- ☐ Interface Ethernet 0
- ☐ Device ID: RTR2611
- ☐ Entry address(es):
- ☐ IP address: 172.10.20.1
- ☐ Platform: cisco 2611, Capabilities: Router
- ☐ Interface Ethernet 0
- ☐ ----------
- ☐ Device ID: C2924C-123
- ☐ Entry address(es):
- ☐ IP address: 10.10.1.3
- ☐ Platform: cisco WS-C2924, Capabilities: Switch
- ☐ Interface Ethernet 0
- ☒ Device ID: RTR2511
- ☒ Entry address(es):
- ☒ IP address: 178.10.20.2
- ☒ Platform: cisco 2511, Capabilities: Router
- ☒ Interface Serial 0
- ☒ ----------
- ☒ Device ID: C2924C-123
- ☒ Entry address(es):
- ☒ IP address: 10.10.1.3
- ☒ Platform: cisco WS-C2924, Capabilities: Switch
- ☒ Interface Ethernet 0
- ☐ Device ID: RTR2611
- ☐ Entry address(es):
- ☐ IP address: 172.10.20.1
- ☐ Platform: cisco 2611, Capabilities: Router
- ☐ Interface Ethernet 0
- ☐ Device ID: C2924C-123
- ☐ Entry address(es):
- ☐ IP address: 10.10.1.3
- ☐ Platform: cisco WS-C2924, Capabilities: Switch
- ☐ Interface Ethernet 0

Explanation:

Explanation:

The following code is the correct partial output of the show cdp neighbors detail command issued on Router A:

Device ID: RTR2511

Entry address(es):

IP address: 178.10.20.2

Platform: cisco 2511, Capabilities: Router

Interface Serial 0

 Licensed to Berend Post berend.post@it-university.nl

Device ID: C2924C-123

Entry address(es):

IP address: 10.10.1.3

Platform: cisco WS-C2924, Capabilities: Switch

Interface Ethernet 0

The show cdp neighbors detail command displays the Cisco devices directly connected to the router. Therefore, only details of the 2511 router and the Cisco Catalyst 2924 switch will be displayed in the output. The detail keyword in the show cdp neighbor command also displays IP address information for the directly connected devices. The output shows the connected device name, its IP address, its platform, and the local interface through which the device is connected.

All of the other code samples are incorrect, as they include the output of devices that are not connected directly to Router A.

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol used by all Cisco devices to collect information about neighboring devices. CDP operates at Layer 2 of the OSI model. Therefore, it can collect information about neighboring devices that are running different Network layer protocols. It is also useful for collecting information when IP is not functional.

Some variations of this command include:

The show cdp command, which displays global CDP information, including timer and hold time information.

The show cdp interface command, which displays information about the interfaces on which CDP is enabled.

The show cdp neighbors command, which displays detailed information about neighboring devices discovered by the CDP. However, it does not include the IP address of the neighboring device.

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Cisco IOS Network Command Reference, Release 12.4 > show cdp neighbors

Question 355

Which two statements represent physical security guidelines that should be followed during Cisco security deployment? (Choose two.)

- ☒ Potential security breaches should be evaluated.
- ☐ Network equipment should be accessed remotely with Secure Socket Layer (SSL) instead of Telnet.
- ☐ Images should be managed using File Transfer Protocol (FTP) and Secure FTP (SFTP) instead of Trivial File Transfer Protocol (TFTP).
- ☐ Simple Network Management Protocol version 3 (SNMPv3) should be used for security and privacy features.
- ☒ The potential impact of stolen network resources and equipment should be assessed.

Explanation:

Explanation:

Potential security breaches should be evaluated and the potential impact of stolen network resources and equipment should be assessed when designing the physical security architecture during Cisco security deployment.

Physical security is considered during security implementation to increase the strength of the complete security design. It helps to protect and limit access to network resources and physical network equipment. The following physical security guidelines should be followed during Cisco security deployment:

Potential security breaches should be evaluated.

The impact of stolen network resources and equipment should be accessed.

Physical access control such as locks and alarms should be used.

To secure traffic flowing on networks outside the user control, a control mechanism such as cryptography should be used.

All the other options are incorrect because they do not represent physical security guidelines. They deal more with the transmission of information and the performance and security implications of that transmission rather than the protection of physical devices.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

 Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Articles > Network Technology > Security > General Design Considerations for Secure Networks

Question 356

Which of the following commands is used to verify the link-local, global unicast, and multicast addresses of an IPv6 router?

- ☐ show ipv6 neighbors (only link-local addresses)
- ☐ show ipv6 route
- ☐ show ipv6 protocols
- ☒ show ipv6 interface

Explanation:

Explanation:

The show ipv6 interface command is used to verify the link-local, global unicast, and multicast addresses assigned to an IPv6-enabled router interface. The show ipv6 interface command displays information regarding that interface, such as the physical state, MTU, and IPv6 enable/disable state.

Here is the partial output of the show ipv6 interface command on an IPv6-enabled router named rtrA:

```
rtrA# show ipv6 interface FastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is
FE80::6339:7BFF:FE5D:A031/64
Global unicast address(es):
2001:7067:90D1:1::1, subnet is 2001:7067:90D1:1/64
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF5D:A031
MTU is 1500 bytes
<output omitted>
```

In the sample output, you can see that the Fa0/1 interface of rtrA has the link-local address FE80::6339:7BFF:FE5D:A031/64 and the global unicast address 2001:7067:90D1:1::1. The global unicast address is not in EUI-64 format because when the ipv6 address command was issued, the eui64 keyword was not used. If the EUI-64 format had been specified with the eui64 keyword, the global unicast address would have been 2001:7067:90D1:1:6339:7BFF:FE5D:A031.

Licensed to Berend Post berend.post@it-university.nl

An IPv6-enabled interface has not only a link-local and global unicast address, but also one or more multicast addresses. A multicast address is an IPv6 address that has the prefix FF00::/8. These addresses are assigned to interfaces of different nodes such that they appear as a logical group. This implies that when a packet is destined for a multicast address, that packet is delivered to all the interfaces that have the same multicast address. The various multicast groups are as follows:

FF02::1 Indicates the group of all the nodes on the local segment

FF02::2 Indicates the group of all the routers on the local segment

FF02::1:FF00:0/104 Indicates a solicited-node multicast group for every unicast or anycast address assigned to the interface

You can also notice in the sample output that the Fa0/1 interface belongs to three multicast groups: FF02::1, FF02::2, and FF02::1:FF5D:A031. The first two multicast groups refer to the all-host and all-router multicast groups, respectively. The third group, FF02::1:FF5D:A031, is the solicited-node multicast address. This address is created for every unicast or anycast address. A solicited-node multicast address is determined by assigning the least significant 24 bits of the unicast address to the least significant 24 bits of the FF02::1:FF00:0 address.

The show ipv6 neighbors command displays the link-local /global unicast addresses of the neighbors, including other information such as state and the next-hop interface.

The show ipv6 route command is used to view the IPv6 routing table on the router. This command displays the prefixes, administrative distance, metric, and 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:

Cisco IOS IPv6 Command Reference > show ipv6 eigrp topology through show ipv6 nat statistics > show ipv6 interface

 Licensed to Berend Post berend.post@it-university.nl

Cisco IOS IPv6 Command Reference > show ipv6 nat translations through show ipv6 protocols > show ipv6 neighbors

Cisco IOS IPv6 Command Reference > show ipv6 nat translations through show ipv6 protocols > show ipv6 protocols

Cisco > Products & Services > Cisco IOS and NX-OS Software > Cisco IOS Technologies > IPv6 > Product Literature > White Papers > Cisco IOS IPv6 Multicast Introduction

Cisco > IPv6 Implementation Guide, Release 15.2M&T > Implementing IPv6 Multicast

Question 357

Which classful protocols perform an automatic summarization of routes when routers send updates across major classful network boundaries? (Choose two.)

- ☒ RIPv1
- ☐ RIPv2
- ☒ IGRP
- ☐ OSPF
- ☐ EIGRP
- ☐ BGPv4

Explanation:

Explanation:

The classful routing protocols Routing Information Protocol version1 (RIPv1) and Interior Gateway Routing Protocol (IGRP) summarize routes at classful network boundaries. RIPv1 is a standard distance vector protocol that uses hop count as a metric. IGRP is a Cisco Systems proprietary distance vector routing protocol that has a composite metric based on bandwidth, delay, load, reliability, and maximum transmission unit (MTU).

In classless routing protocols RIPv2, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP) and Border Gateway Protocol version 4 (BGPv4), route summarization can be controlled manually at any bit position in the IP address. Classless routing protocols transmit subnet mask along with the routes, and therefore manual summarization may be required at times to keep the routing table size in control.

It should be noted that RIPv2 and EIGRP, although classless protocols, will perform automatic summarization by default unless the no auto-summary command is configured. Once no auto-summary is configured, you can manually configure summarization on any bit position in the IP address. Since you can override auto-summarization in both RIPv2 and EIGRP, RIPv1 and IGRP are better answers to this question.

Objective:

 Licensed to Berend Post berend.post@it-university.nl

Routing Fundamentals

Sub-Objective:

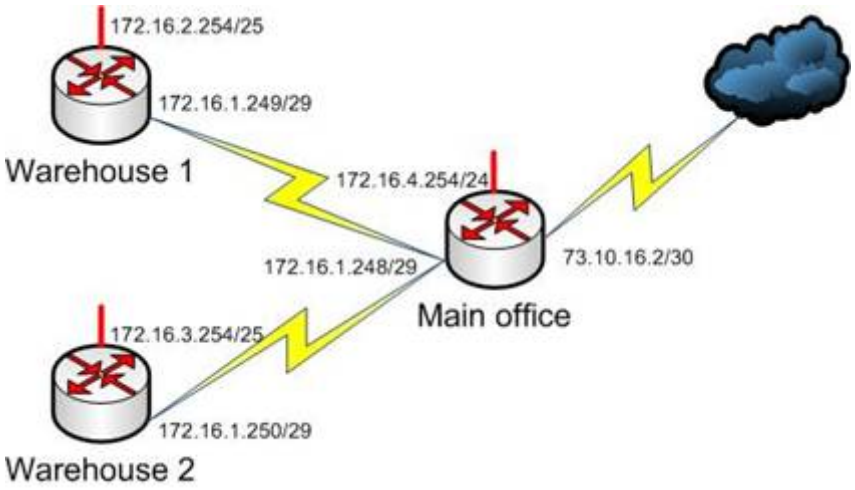
Compare and contrast interior and exterior routing protocols

References:

Cisco > Articles > Cisco Networking Academy > CCNP 1: Advanced IP Addressing Management

Question 358

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?

- ☐ Change the IP address of the Warehouse 1 LAN interface.
- ☐ Change the IP address of the Warehouse 1 WAN interface.
- ☐ Change the IP address of the Main Office LAN Interface.
- ☒ Change the IP address of the Main Office WAN interface.
- ☐ Change the IP address of the Main Office Internet interface.

Explanation:

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:

Licensed to Berend Post berend.post@it-university.nl

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:

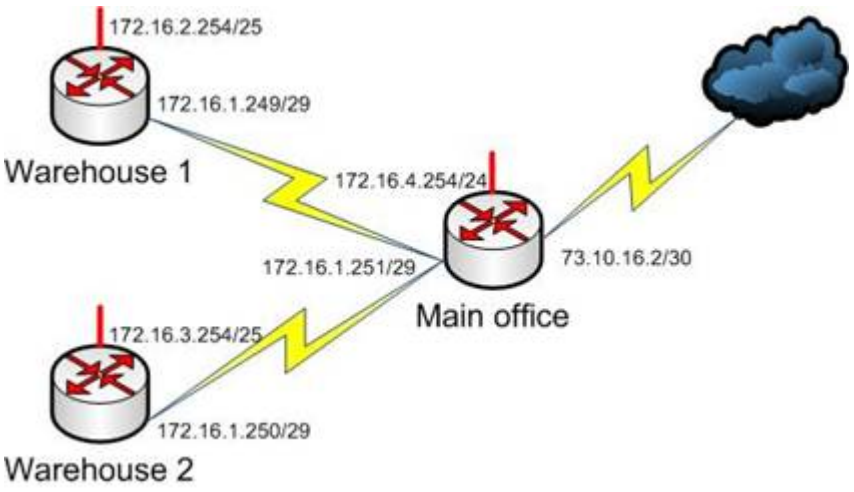
172.16.1.240

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:



Licensed to Berend Post berend.post@it-university.nl

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

IP Addressing and Subnetting for New Users

Question 359

Which of the following statements are TRUE regarding EIGRP operation? (Choose two.)

- ☐ A successor is a backup route, and is installed in both the routing and topology tables.
- ☒ A successor is a primary route, and is installed in both the routing and topology tables.
- ☐ A successor is a primary route, and is installed only in the routing table.
- ☐ A feasible successor is a backup route, and is installed in both the routing and topology tables.
- ☐ A feasible successor is a primary route, and is only installed in the routing table.
- ☒ A feasible successor is a backup route, and is only installed in the topology table.
- ☐ If the successor route fails and no feasible successor route exists, the router will send an update with the route marked with an unreachable metric of 16.

Explanation:

Explanation:

In EIGRP operations, primary or active routes are known as successors. These routes are maintained in both the routing and topology tables. The routing table is the list of network paths that are currently used by the router.

EIGRP also has the ability to maintain backup routes to destination networks. These backup routes are known as feasible successors. If a feasible successor is discovered by EIGRP, it will be maintained only in the topology table, since it is not currently being used to route traffic. In the event of a successor failure, the backup feasible successor will become the successor, and will be installed in the routing table automatically. If the successor route fails and no feasible successor route exists, the router will send queries to all neighbors until a new successor is found.

EIGRP maintains three dynamic tables in RAM:

Neighbor table, which is a list of all neighboring EIGRP routers on shared subnets

Topology table, which contains all discovered network paths in the internetwork

 Licensed to Berend Post berend.post@it-university.nl

Routing table, which contains the best path (based on lowest metric) to each destination network

A successor is not a backup route. A successor is a primary or active route, and it is stored in both the routing and topology tables.

A feasible successor is not a primary route. It is a backup route, and it is stored only in the topology table.

If the successor route fails and no feasible successor route exists, the router will not send an update with the route marked with an unreachable metric of 16. EIGRP does not send an update with the route marked with an unreachable metric, and even if it did, 16 is not an unreachable metric in EIGRP as it is in RIP. Instead it sends a multicast query packet to all adjacent neighbors requesting available routing paths to the destination network.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > Enhanced Interior Gateway Routing Protocol > Document ID: 16406 > Feasible Distance, Reported Distance, and Feasible Successor

Question 360

Which command enables HSRP on an interface?

- ☐ hsrp
- ☒ standby ip
- ☐ standby mode hsrp
- ☐ switchport mode hsrp

Explanation:

Explanation:

The standby ip interface configuration command enables Hot Standby Router Protocol (HSRP). The syntax for this command is as follows:

Licensed to Berend Post berend.post@it-university.nl

switch(config-if)# standby group-number ip ip-address

The group-number argument specifies the HSRP group number on the interface. You do not need to enter a group number if there is only one HSRP group.

At least one interface on one of the routers in the group must be configured with the virtual IP address of the group. It is optional on all other interfaces on the other routers, which can learn the address through the hellos sent among the group.

A complete HSRP configuration is shown below with an explanation of each command.

RouterA (config) #interface Fa0/1

RouterA (config-if) # ip address 192.168.5.6 255.255.255.0

RouterA (config-if) # standby 2 ip 192.168.5.10

RourerA(config-if) # standby 2 priority 150

RouterA (config-if) #standby 2 Preempt

RouterA(config-if) #standby 2 track interface fa0/2

Line 1 specifies the interface

Line 2 addresses the interface

Line 3 specifies the HSRP group number and the virtual IP address

Line 4 sets the HSRP priority

Line 5 allows the router to take the active role if its priority becomes higher than that of the active router

In the above, the router is tracking its own Fa0/2 interface. If that interface goes down it will reduce its priority by 10 (this is the default decrement when not specified). The new value would be 140 if that happened. To specify a decrement value, add it to the track command, as in this example: track interface Fa0/2 20.

When you configure routers to be part of an HSRP group, they listen for the HSRP MAC address for that group as well as their own burned-in MAC addresses.

HSRP uses the following MAC address:

0000.0c07.ac** (where ** is the HSRP group number)

 Licensed to Berend Post berend.post@it-university.nl

The switchport mode interface configuration command will configure the VLAN membership mode of a port. It is not used to enable HSRP.

The options standby mode hsrp and hsrp are not valid commands.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco > Home > Technology Support > IP > IP Application Services > Design > Design Technotes > Hot Standby Router Protocol Features and Functionality

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

Question 361

Which statement is TRUE regarding the switchport protected interface configuration command and its effects?

- ☒ The command is used to configure private VLAN edge ports.
- ☐ The command enables the highest level switch port security.
- ☐ All the traffic through protected port should go via a Layer 2 device such as switch.
- ☐ A protected port can directly communicate with any other port on the same switch.

Explanation:

Explanation:

The switchport protected interface configuration command is used to configure private VLAN edge ports on a Cisco Catalyst 2950 switch. A VLAN edge port is another name given to a protected port. Protected ports do not forward any traffic to other protected ports on the same switch. All traffic passing between protected ports on the same switch must be routed through a Layer 3 device. Protected ports have no restrictions on forwarding to non-protected ports, and they forward as usual to all ports on other switches

Following are the steps to configure a switch port as a protected port:

1. configure terminal

 Licensed to Berend Post berend.post@it-university.nl

2. interface interface-id

3. switchport protected

4. end

Use the show interfaces switchport command to verify that the protected port is enabled.

It is incorrect to state that the command enables the highest level of switch port security. It places no additional restrictions on the port other than preventing it from directly forwarding from one protected port to another.

It is incorrect to state that all traffic through protected port should go via a Layer 2 device such as a switch. Traffic through the protected port should go via a Layer 3 device, such as a router.

It is incorrect to state that a protected port can directly communicate with any other port on the same switch. A protected port cannot directly communicate with another protected port on the same switch.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

Cisco > Catalyst 2960 Switch Command Reference, 12.2(44)SE > Catalyst 2960 Switch Cisco IOS Commands - shutdown through vtp > switchport protected

Question 362

Which Cisco IOS command is used to view the information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled?

- ☒ show cdp interface
- ☐ show interfaces
- ☐ show cdp
- ☐ show cdp interfaces

Explanation:

Explanation:

 Licensed to Berend Post berend.post@it-university.nl

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

Licensed to Berend Post berend.post@it-university.nl

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

 Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Cisco IOS Network Management Command Reference > show cdp interface

Question 363

Which two features do Cisco routers offer to mitigate distributed denial-of-service (DDoS) attacks? (Choose two.)

- ☐ Anti-DDoS guard
- ☐ Scatter tracing
- ☒ Access control lists (ACLs)
- ☐ Flow control
- ☒ Rate limiting

Explanation:

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.

 Licensed to Berend Post berend.post@it-university.nl

Anti-DDoS guard and scatter tracing are incorrect because these features are not offered by Cisco routers to mitigate DDoS attacks.

Flow control is incorrect because flow control is used to prevent the loss of traffic between two devices.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Support > Technology Support > Security and VPN > Authentication Protocols > Technology Information > Technology White Paper > Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks > Document ID: 13634

Question 364

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.)

- ☐ The router's serial interface is connected using a DTE cable.
- ☒ The router's serial interface is connected using a DCE cable.
- ☒ The router's serial interface is administratively down.
- ☐ The router's serial interface connects using the point-to-point protocol.

Explanation:

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.

 Licensed to Berend Post berend.post@it-university.nl

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 365

How is the designated router (DR) determined by OSPF on a multi-access network segment?

- ☐ The lowest interface priority, then the highest RID
- ☒ The highest interface priority, then the highest RID
- ☐ The lowest interface priority, then the highest OSPF process ID
- ☐ The highest interface priority, then the highest OSPF process ID

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

OSPF routers elect a designated router (DR) and backup designated router (BDR) on multi-access network segments in order to minimize the amount of update traffic sent between OSPF neighbors. All routers on multi-access network segment form adjacencies with the DR and BDR, but not with each other. Network events are communicated to the DR, and the DR distributes the event to the rest of the network.

The DR is determined by the router with the highest interface priority number. If the priority numbers tie (which will be the case if they are left to the default of 1), then the router with the highest router ID (RID) becomes the DR. The default priority number is 1, and can be configured as high as 255.

In many cases, it is desirable to intervene in this process and select the router you want to be the DR. If that is the case and the selected router is not becoming the DR for whatever reason, the following options are available to ensure that the selected router wins the election:

Change the priority value of the router to a value higher than the other routers

Set the priority value of the other routers to 0

Create a loopback address on the selected router with an IP address higher than the IP addresses used on the other routers

Changing the priority to 0 makes the router ineligible to become the DR or BDR. The ip ospf priority # command is used to manually configure a priority on a specific interface.

It is also worth noting that a single OSPF area can have more than one DR. The election is NOT performed per area, but per network segment. So if you had six OSPF routers in area 0 with three in one IP subnet and three in another, there would be two elections, one for each segment.

The lowest interface priority does not determine the DR.

The OSPF process ID has no effect on DR elections.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039 > DR Election

Question 366

Which type of connector is used for an Integrated Services Digital Network Basic Rate Interface (ISDN BRI) connection?

- ☐ DB-60
- ☒ RJ-45
- ☐ AUI
- ☐ Console

Explanation:

Explanation:

An RJ-45 connector is used for an ISDN BRI connection. A BRI port is used in order to connect an asynchronous BRI interface.

The DB-60 option is incorrect because the DB-60 connector is used to provide connectivity between synchronous serial interfaces and Cisco routers. The serial ports are used to connect with the synchronous serial interfaces. DB-60 serial ports are used for Wide Area Network (WAN) connections. High-speed lines (E1 or T1) can be configured using serial ports.

The AUI option is incorrect because the AUI connector is used with Ethernet ports.

The console option is incorrect because console port enables device management. It provides out-of-band access to the router command line interface.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco Tech Notes > Cabling Guide for Console and AUX Ports > Document ID: 12223

http://www.tutorialsweb.com/networking/routers/cisco-rotuers-ios.htm#Hardware%20Components:

Licensed to Berend Post berend.post@it-university.nl

Question 367

Which two modes are Cisco Internetwork Operating System (IOS) operating modes? (Choose two.)

- ☐ User Privileged mode
- ☒ User EXEC mode
- ☐ Local configuration mode
- ☒ Global configuration mode
- ☐ NVRAM monitor mode

Explanation:

Explanation:

User EXEC mode and global configuration mode are the Cisco IOS operating modes. The following list shows the Cisco IOS operating modes along with their description:

User EXEC mode: The commands in this mode are used to enable connections to remote devices and change the terminal settings for a short duration. User EXEC commands also enable you to perform basic tests and view system information.

Global configuration mode: The commands in this mode enable you to make changes to the entire system.

Privileged EXEC mode: The commands in this mode are used to configure operating parameters. This mode also provides access to the remaining command modes.

Interface configuration mode: The commands in this mode allow you to change the operation for interfaces such as serial or Ethernet ports.

ROM monitor: The commands in this mode are used to perform low-level diagnostics.

All the other options are incorrect because they are not valid Cisco IOS operating modes.

To enter privileged EXEC mode, you must enter the command enable on the router. You will then be prompted for the enable password, if one has been created.

To enter global configuration mode, you must first enter privileged EXEC mode (see above) and then enter the command configure terminal (which can be abbreviated to config t), and the router will enter a mode that allows you to make global configuration changes.

Objective:

Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco Documentation > RPM Installation and Configuration > IOS and Configuration Basics > Cisco IOS Modes of Operation

Question 368

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?

- ☒ no cdp run
- ☐ set cdp disable
- ☐ no cdp enable
- ☐ no cdp advertise-v2

Explanation:

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:

 Licensed to Berend Post berend.post@it-university.nl

Cisco > Support > Using Cisco Discovery Protocol

Cisco > Support > Technology Support > Network Management > Cisco's Response to the CDP Issue > Document ID: 13621

Question 369

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
```

- ☐ 192.168.1.10
- ☒ 192.168.4.2
- ☐ 192.168.10.254
- ☐ None; the packet will be dropped.

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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.

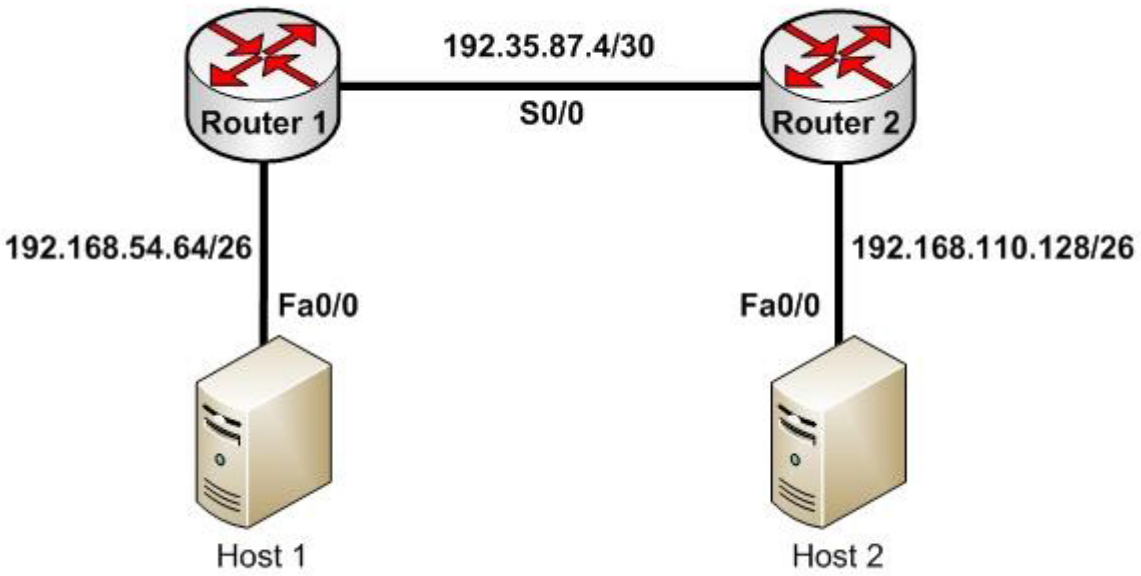
To ensure that no packets are dropped, even if there is no matching route in the routing table, a default route could be configured as follows (next hop picked at random for illustration):

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:

Licensed to Berend Post berend.post@it-university.nl




```
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:

Licensed to Berend Post berend.post@it-university.nl

Interpret the components of routing table

References:

Cisco > Support > IP > IP Routing > Design > Design TechNotes > Route Selection in Cisco Routers > Document ID: 8651

Question 370

Which Cisco command keeps unauthorized users from viewing passwords in the router configuration file?

- ☐ enable secret
- ☐ enable password
- ☐ enable encryption
- ☐ service encryption
- ☒ service password-encryption

Explanation:

Explanation:

The service password-encryption global configuration mode command keeps unauthorized users from viewing passwords in the router configuration file. The service password-encryption command encrypts all current and future passwords configured on the router, including the line password, virtual terminal password, console password, user name password, routing protocol passwords such as BGP neighbor passwords, the privileged command password, and authentication key passwords. Moreover, it encrypts any future passwords created on the router.

The encryption process occurs whenever the current configuration is built or a password is configured. The service password-encryption command will cause the router configuration file to display encrypted characters instead of passwords when the running-configuration or startup-configuration files are viewed.

The enable password command creates a password that will be required to enter privileged EXEC mode, but the password will not be encrypted.

The enable secret command provides encryption to the enable mode passwords but does not apply globally to all passwords configured on the router. It also does not encrypt any future passwords created on the router.

The enable encryption and service encryption commands are invalid.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Cisco IOS Security Command Reference > service password-encryption

Cisco Tech Notes > Cisco IOS Password Encryption Facts > Document ID: 107614

Question 371

What is the valid host address range for the subnet 172.25.4.0 /23?

- ☒ 172.25.4.1 to 172.25.5.254
- ☐ 172.25.4.10 to 172.25.5.210
- ☐ 172.25.4.35 to 172.25.5.64
- ☐ 172.25.4.21 to 172.25.5.56

Explanation:

Explanation:

For the subnet 172.25.4.0, the valid host range will start at 172.25.4.1 and end at 172.25.5.254.

To determine the valid range of addresses in a subnet, one must determine the subnet number or network ID and the broadcast address of the subnet and all valid addresses will lie within those boundaries.

In this case:

Network address: 172.25.0.0

Subnet mask in decimal: 255.255.254.0 (/23 indicates 23 bit in the mask)

Subnet mask in binary: 11111111.11111111.11111110.00000000

The formulas to calculate the number of subnets and hosts are:

Number of subnets = 2number-of-subnet-bits

Number of hosts per subnet = 2number-of-host-bits - 2

In this scenario:

 Licensed to Berend Post berend.post@it-university.nl

Number of subnet bits: 7 (the binary 1s in the third octet of the subnet mask)

Number of subnets: 27 = 128

Number of host bits: 9 (the binary 0s in the subnet mask)

Number of hosts: 29 - 2 = 510

These formulas are useful when determining if a subnet mask/network ID combination will support a given number of hosts.

To determine the boundaries of each of the 128 subnets that this mask will yield, you should utilize a concept called the interval or block size. This number helps to identify the distance between network IDs. Determining the network IDs allows the identification of the broadcast address for each subnet, because the broadcast address for any particular subnet will always be the last address before the next network ID. The interval is determined by the value of the far right-hand bit in the mask, which is 2 in this case. Then it is applied to the octet where the mask ends. In this case, the first 4 network IDs are:

172.25.0.0

172.25.2.0

172.25.4.0

172.25.6.0

...incrementing by two at each point

Therefore, the valid addresses in the 172.25.4.0 network are framed by the two addresses that cannot be used: 172.25.4.0 (network ID) and 172.25.5.255 (broadcast address, or the last address before the next network ID). The addresses within these boundaries are 172.25.4.1 to 172.25.5.254.

For subnet 172.25.0.0, the valid host range will run from 172.25.0.1 to 172.25.1.254. The broadcast address for subnet 172.25.0.0 will be 172.25.1.255.

For subnet 172.25.2.0, the valid host range will run from 172.25.2.1 to 172.25.3.254. The broadcast address for subnet 172.25.2.0 is 172.25.3.255.

For the subnet 172.25.4.0, the valid host range will run from 172.25.4.1 to 172.25.5.254. The broadcast address for subnet 172.25.4.0 is 172.25.5.255.

Licensed to Berend Post berend.post@it-university.nl

Always remember that the first address of each subnet is the network ID, and as such cannot be used as a host or router IP address. Also, the last address of each subnet is the broadcast address for the subnet, and as such cannot be used as a host or router IP address.

Objective:

Network Fundamentals

Sub-Objective:

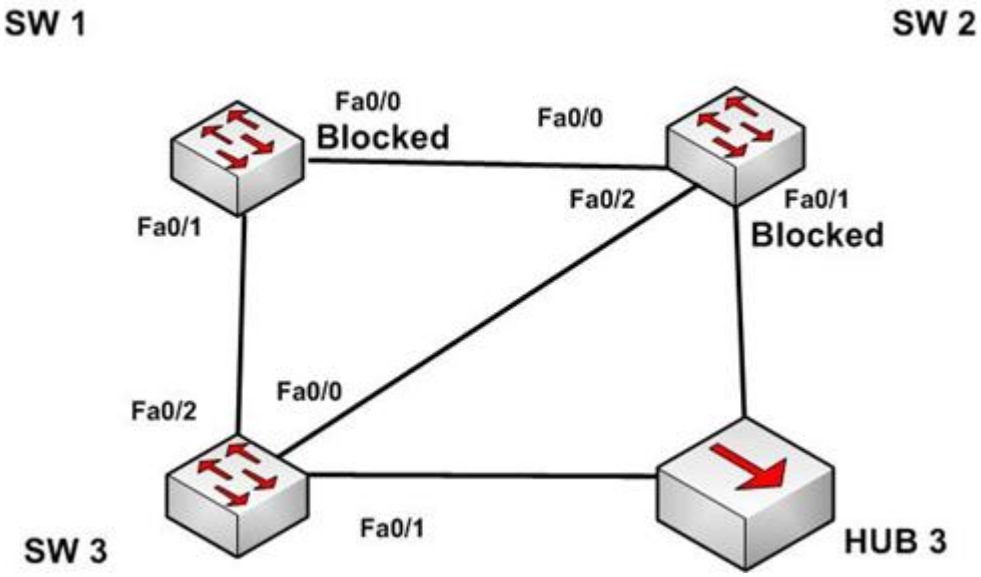
Compare and contrast IPv4 address types

References:

Cisco > Support > Technology Support > IP > IP Routing > Design > Design Technotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Question 372

The diagram below shows the state of the switch interfaces after STP has converged.



Based on the interface states, which of the following statements are true? (Choose all that apply.)

- ☐ The Fa0/2 interface on SW 2 is a designated port
- ☒ SW 3 is the root bridge
- ☐ SW 2 is the root bridge
- ☒ The Fa0/0 interface on SW 2 is a designated port
- ☐ The Fa0/0 interface on SW 2 is a root port

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Convergence has occurred in a spanning-tree network when all switch ports are in either a forwarding state or a blocking state (known as discarding state in RSTP). You can use the location of these blocked and forwarding ports to infer the location of the root bridge and the state of any unlabeled ports in the diagram.

SW3 is the root bridge and the Fa0/0 interface on SW2 is a designated port. It can be determined that SW3 is the root bridge because all of its ports are in a forwarding state. Any switch that has at least one port blocking (such as SW1 and SW2) are non-root bridges. As there must be a root bridge, that leaves SW3 as the only candidate.

After establishing that SW3 is the root, it can be determined that the connection between SW1 and SW2 is a segment that does not have a direct connection to the root bridge. These sections must have one end set as a designated port and thus set to forward. Since the Fa0/0 interface on SW2 is forwarding, it is the designated port for that segment.

The Fa0/2 interface on SW2 is not a designated port. The interface on each non-root switch with the lowest cost path to the root bridge will be the root port. Since SW3 is the root bridge, the connection to SW3 via Fa0/2 is the lowest cost path to the root bridge for SW1 and thus is a root port, not a designated port. Moreover, designated ports only exist on segments that do not have a direct connection to the root bridge.

SW2 is not the root bridge. One of its ports is blocking, which will not occur on a root bridge.

The Fa0/0 interface on SW2 is a not root port. It is the designated port for the segment between SW1 and SW2.

The process of determining these port states occurs in this order:

Selection of the root bridge. When all bridge priorities have been left to their default, all switches will have same bridge priority. When that is the case, the switch with the lowest MAC address will be selected root bridge. ALL ports are in a forwarding state on the root bridge, which explains why all of the ports on SW3 will be in a forwarding state.

Determination of the root ports on each non-root bridge. Each non-root bridge will select the interface it possesses with the least cost path to the root bridge. Once selected, that port will be placed in a forwarding state.

Determination of the designated port on each segment that does not connect directly to the root bridge. There is one such segment in the diagram (SW1 to SW2). The interface on either end of the segment that has the least cost path to the root bridge will be the designated port for that section. It

Licensed to Berend Post berend.post@it-university.nl

may have several paths, but the least cost path is used in the determination of the designated port for the segment.

Once determined, the designated ports will be set to forwarding, and all ports that are neither root nor designated ports will be set to blocking.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Internetworking Technology Handbook > Bridging and Switching > Transparent Bridging > Spanning-Tree Algorithm

Question 373

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?

- ☐ CSMA/CA
- ☒ CSMA/CD
- ☐ CSMA/CB
- ☐ CSMA/CS

Explanation:

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 transmit at once, resulting in collisions. If a collision occurs, the transmitting stations perform a

 Licensed to Berend Post berend.post@it-university.nl

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:

Cisco Documentation > Internetwork Troubleshooting Handbook > Troubleshooting Ethernet

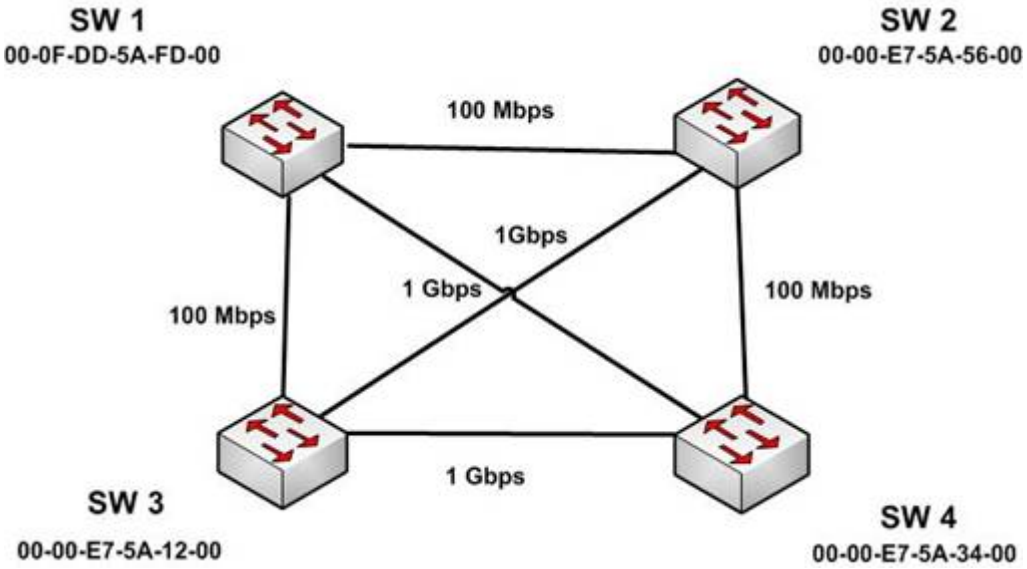
Cisco > Tech Notes > Troubleshooting Ethernet Collisions > Document ID: 12768

Cisco > Technology Support > Ethernet > Carrier Sense Multi-Access/Collision Detection (CSMA/CD)

Licensed to Berend Post berend.post@it-university.nl

Question 374

The four switches in the diagram below have default configurations. Considering the bandwidths indicated on each link and the MAC addresses indicated for each switch, which ports will be forwarding after RSTP has converged? (Choose all that apply.)



- ☒ SW 1 port that connects to SW 4
- ☐ SW 1 port that connects to SW 2
- ☐ SW 1 port that connects to SW 3
- ☒ SW 2 port that connects to SW 3
- ☐ SW 2 port that connects to SW 4
- ☒ SW 3 port that connects to SW 4
- ☒ SW 3 port that connects to SW 1
- ☒ SW 3 port that connects to SW 2

Question 375

Which two security features can be configured to prevent unauthorized access into the network through a networking device? (Choose two.)

- ☐ Anti-Replay
- ☒ Traffic filtering
- ☒ Authentication
- ☐ IPSec network security

Explanation:

Explanation:

Traffic filtering and authentication security can be configured to prevent unauthorized access into the network through a networking device. Unauthorized access to the company's network should be blocked because unauthorized access can damage a company's network. Attackers may access confidential data, plant a virus in the network, or flood the network with illegitimate packets. Therefore, preventive measures should be taken to block any unauthorized access.

Licensed to Berend Post berend.post@it-university.nl

The traffic filtering security feature uses two measures to prevent unauthorized access into the network: access lists and Cisco IOS firewalls.

Access lists are configured to determine which traffic to block and which traffic should be forwarded at the router interfaces. The following types of access lists are available when using Cisco devices:

Basic access lists: Allow only specific traffic through the device; other traffic is dropped.

Extended access lists: Used to filter the traffic based on source IP address, destination IP address, port numbers, or protocols.

Cisco IOS firewalls provide various security features according to your needs. Following are the key components of Cisco IOS firewall:

Context-based Access Control (CBAC): Filters TCP and UDP packets on the basis of application layer protocol session information.

Cisco IOS firewall Intrusion Detection System (IDS): Used to detect suspicious activity. IDS are used to watch packets and sessions as they flow through the router and scan then to match IDS signatures. If the packet is detected as suspicious, the packet is dropped.

Authentication Proxy: Used to apply specific security policies on a per-user basis.

Authentication security can be used to prevent unauthorized access to the network. When a user attempts to access a service or host within the network, they must enter credentials such as their user name and password. If the credentials are correct, then access is provided; otherwise, the user is not allowed to access the service.

Anti-replay and IPSec network security cannot prevent unauthorized access through a networking device into the network. Anti-replay prevents the capture and replay of packets on a network. Although a good security feature to deploy it does not specifically address access to the network through a device. IPSec is used to encrypt and protect the integrity of data that travels through the network, not control access through a device.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Tech Notes > Cisco Guide to Harden Cisco IOS Devices > Document ID: 13608

Licensed to Berend Post berend.post@it-university.nl

Question 376

You want to encrypt and transmit data between peer routers with high confidentiality. Which protocol option should you choose?

- ☐ Authentication Header (AH) in tunnel mode
- ☐ Authentication Header (AH) in transport mode
- ☒ Encapsulating Security Payload (ESP) in tunnel mode
- ☐ Encapsulating Security Payload (ESP) in transport mode

Explanation:

Explanation:

You should choose Encapsulating Security Payload (ESP) in tunnel mode to encrypt and transmit data between peer routers with high confidentiality. Two protocols can be used to build tunnels and protect data traveling across the tunnel:

Authentication Header (AH) uses protocol 51.

ESP uses protocol 50.

AH is defined in Request for Comments (RFC) 1826 and 2402. AH does not perform data encryption and therefore, information is passed as clear text. The purpose of AH is to provide data integrity and authentication, and anti-reply service (optional). It ensures that a packet that crosses the tunnel is the same packet that left the peer device and no changes have been made. It uses a keyed hash to accomplish this.

ESP is defined in RFC 2406. ESP can provide data integrity and authentication, but its primary purpose is to encrypt data crossing the tunnel. There are two reasons why ESP is the preferred building block of IPSec tunnels:

The authentication component of ESP does not include any Layer 3 information. Therefore, this component can work in conjunction with a network using Network Address Translation (NAT).

On Cisco devices, ESP supports encryption using Advanced Encryption Standard (AES), Data Encryption Standard (DES), or Triple DES (3DES).

Tunnel mode is used between Virtual Private Network (VPN) gateways such as routers, firewalls, and VPN concentrators.

Transport mode is used between end-stations or between an end-station and a VPN gateway.

The options AH in tunnel mode and AH in transport mode are incorrect because AH does not provide encryption.

Licensed to Berend Post berend.post@it-university.nl

The option ESP in transport mode is incorrect because transport mode is used between end-stations or between an end-stations and a VPN gateway.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco > Articles > Network Technology > General Networking > IPSec Overview Part Two: Modes and Transforms

Cisco > The Internet Protocol Journal > The Internet Protocol Journal - Volume 3, No. 1, March 2000 > IP Security

Question 377

Which of the following is NOT true of the Cisco APIC-EM?

- ☐ It can verify the operation of access lists
- ☐ It provides network topology visualization
- ☐ It can perform identity tracking
- ☒ It is appropriate for the datacenter environment

Explanation:

Explanation:

With all of its benefits, the Cisco APIC-EM is not appropriate for the datacenter environment. A more appropriate controller for the datacenter environment is Cisco APIC-DC. Both of these are software-defined network controllers, which can be used to program a network in an automated fashion.

Specific benefits provided by the Cisco APIC-EM include:

It can verify the operation of access lists with the Path Trace Analysis tool

It provides network topology visualization

It can perform identity tracking

It provides an inventory of devices

It automatically adds new devices

Objective:

 Licensed to Berend Post berend.post@it-university.nl

Infrastructure Security

Sub-Objective:

Verify ACLs using the APIC-EM Path Trace ACL analysis tool

References:

Performing Path Traces

Question 378

You are the network administrator for your company. You want to upgrade the network, which is currently running on IPv4, to a fully functional IPv6 network. During the transition, you want to ensure that hosts capable only of IPv6 can communicate with hosts capable only of IPv4 on the network.

Which solution should you implement to accomplish the task in this scenario?

- ☐ IPv6 over IPv4 tunnels
- ☐ IPv6 over dedicated Wide Area Network (WAN) links
- ☐ Dual-Stack Backbones
- ☒ Protocol translation

Explanation:

Explanation:

The protocol translation deployment model should be used to accomplish the task in this scenario. It is the only offered solution that does not require at least one end of the communication solution to support both IPv6 and IPv4.

The following deployment models are available for IPv4 to IPv6 migration:

IPv6 over IPv4 tunnels: IPv6 traffic is encapsulated into IPv4 packets. Then these packets are transferred over IPv4 WAN. This model eliminates the need to create separate circuits to connect to the IPv6 networks. This model increases protocol overhead because of the IPv6 headers and requires the edge router at each end be capable of both protocols.

Protocol translation: A method allowing an IPv6 host to communicate with an IPv4 host. This is accomplished with the help of Network Address Translation - Protocol Translation (NAT-PT) used to configure translation between IPv6 and IPv4 hosts. NAT-PT allows communication between IPv6 hosts and applications, and native IPv4 hosts and applications.

IPv6 over dedicated WAN links: A new deployment of IPv6 is created. In this model, IPv6 hierarchy, addressing, and protocols are used by all nodes. However, this model involves cost for creating IPv6 WAN circuits. This solution is not designed for LAN translation but rather communication over WAN links.

Licensed to Berend Post berend.post@it-university.nl

Dual-Stack Backbones: A hybrid model in which backbone routers have dual-stack functionality, which enables them to route both IPv4 and IPv6 packets. It is suitable for an enterprise that uses both IPv4 and IPv6 applications. Running IPv6 and IPv4 together in a network is known as dual-stack routing.

Objective:

Network Fundamentals

Sub-Objective:

Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment

References:

Cisco > Products and Services > Security > Cisco IOS Network Address Translation (NAT) > Data Sheets and Literature > White Papers > Network Address Translator-Protocol Translator

Question 379

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.)

- ☒ Check the cable connections.
- ☒ Reset the equipment.
- ☐ Check the router configuration.
- ☐ Check the router configuration for the shutdown interface command.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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:

Cisco > Cisco IOS Interface and Hardware Component Command Reference > show interfaces summary

Cisco Documentation > Cisco 1700 Series Router Software Configuration Guide > Configuring a Leased Line > Troubleshooting Problems with Leased Lines

Licensed to Berend Post berend.post@it-university.nl

Question 380

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?

- ☐ 192.168.144.23
- ☐ 192.168.144.28
- ☒ 192.168.144.31
- ☐ 192.168.144.32

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Cisco > Technology Support > IP > IP Routing > Design TechNotes > IP Addressing and Subnetting for New Users > Document ID: 13788 > Understanding IP Addresses

Question 381

Which commands would you use to determine the IP address and hostname of a directly connected switch from which you received VLAN information? (Choose two. Each correct answer is part of the solution.)

- ☒ show vtp status
- ☒ show cdp neighbors detail
- ☐ show cdp neighbor status
- ☐ show vtp counters
- ☐ show cdp neighbor

Explanation:

Explanation:

The VLAN Trunking Protocol (VTP) is used to synchronize VLANs between switches, and the question implies that VTP is being used in this environment. The show vtp status command will display the IP address of the switch that last updated your VLAN database. The output of this command is as follows:

```
Switch# show vtp status
VTP Version : 2
Configuration Revision : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs : 33
VTP Operating Mode : Server
VTP Domain Name : Lab_Network
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 10.1.1.2 at 8-12-99 15:04:49
<output omitted>
```

The "Configuration last modified by 10.1.1.2" output reveals the IP address of the switch from which you received VLAN information. Once you know the IP address of the switch, you can use the show

 Licensed to Berend Post berend.post@it-university.nl

cdp neighbors detail command to determine the hostname associated with this IP address. The output of this command is as follows:

```
switch# show cdp neighbors detail
Device ID: RouterB
Entry address(es):
IP address: 172.20.52.254
Platform: cisco 2621, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port):
FastEthernet0/0
Holdtime: 120 sec
<<output omitted>>

-------------------------------------------------

Device ID: SwitchB
Entry address(es):
IP address: 10.1.1.2
Platform: cisco WS-C2950G-24, Capabilities: Switch IGMP
Interface: FastEthernet0/4, Port ID (outgoing port):
FastEthernet0/24
Holdtime: 101 sec
<<output omitted>>
```

The show cdp neighbors detail command provides detailed information about directly connected Cisco devices. The detail option is required to provide the IP address of the neighboring devices, and indicates here that IP address 10.1.1.2 is assigned to Device ID: SwitchB, which is the hostname for this device. SwitchB is the switch from which you received VLANs.

Although not offered as an option, the show cdp entry* command will also display all directly connected devices and will indicate the hostname and the IP address and platform, but will not indicate from which device VTP information was received. Its output is shown below:

```
switch#show cdp entry*
-----------------------

Device ID: SwitchB
Entry address(es):
IP address: 10.1.1.2
Platform: cisco WS-C2950G-24, Capabilities: Switch IGMP
Interface: FastEthernet0/4, Port ID (outgoing port):
FastEthernet0/24
Holdtime: 101 sec
<<output omitted>>
```

This command displays the same information as the show cdp neighbor detail command. It includes:

Licensed to Berend Post berend.post@it-university.nl

The IP address of the neighbor (in this case 10.1.1.2)

The port on which the CDP information was received (in this case FastEthernet0/4)

The platform (in this case a Cisco WS-C2950G-24 Switch)

The show vtp counters command is incorrect because it does not display information about neighboring devices, nor information regarding from which switch VLANs were received.

The show cdp neighbor command is incorrect because the detail option is required to display the IP addresses of neighboring devices.

The show cdp neighbor status command is incorrect because this is not a valid Cisco IOS command.

Objective:

LAN Switching Fundamentals

Sub-Objective:

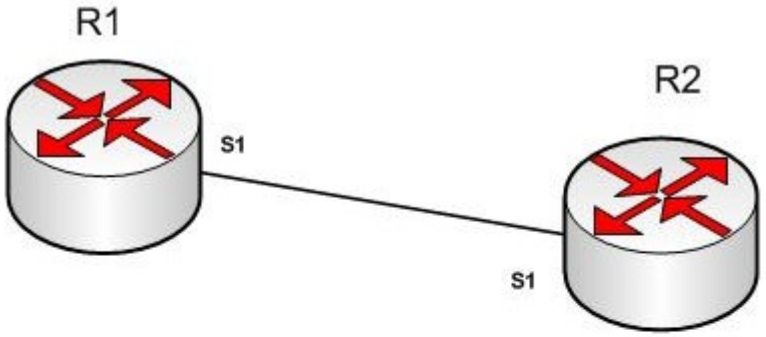
Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Licensed to Berend Post berend.post@it-university.nl

Question 382

R1 and R2 are connected as shown in the diagram and are configured as shown in output in the partial output of the show run command.




```
R1#show run

version 12.0
hostname R1

interface s1
ip address 192.168.5.5 255.255.255.252

ip host R1 192.168.5.6

R2#show run

version 12.0
hostname R2
interface s1
ip address 192.168.5.6 255.255.255.252
ip host R1 192.168.5.5
```

The command ping R2 fails when executed from R1. What command(s) would allow R1 to ping R2 by name?

- ☐ R1(config)#int S1
- ☐ R1(config-if)#no ip address 192.168.5.5
- ☐ R1(config-if)# ip address 192.168.5.9 255.255.255.252
- ☒ R1(config)#no ip host R1
- ☒ R1(config)# ip host R2 192.168.5.6 255.255.255.252
- ☐ R1(config)#no hostname R2
- ☐ R1(config)# hostname R1
- ☐ R2(config)#int S1
- ☐ R1(config-if)#no ip address 192.168.5.5
- ☐ R1(config-if)# ip address 192.168.5.9 255.255.255.0

Explanation:

Explanation:

Both routers have been configured with the ip host command. This command creates a name to IP address mapping, thereby enabling the pinging of the device by address. On R1, the mapping is

Licensed to Berend Post berend.post@it-university.nl

incorrect and needs to be corrected. Currently it is configured as ip host R1 192.168.5.6. It is currently mapping its own name to the IP address of R2.

To fix the problem, you should remove the incorrect IP address mapping and create the correct mapping for R2, as follows:

R1(config)#no ip host R1

R1(config)# ip host R2 192.168.5.6 255.255.255.252

Once this is done, the ping on R2 will succeed.

The IP address of the S1 interface on R1 does not need to be changed to 192.168.5.9 /30. In fact, if that is done the S1 interface on R1 and the S1 interface in R2 will no longer be in the same network. With a 30-bit mask configured, the network they are currently in extends from 192.168.5.4 - 192.168.5.7. They are currently set to the two usable addresses in that network, 192.168.5.5 and 192.168.5.6.

The hostnames of the two routers do need to be set correctly using the hostname command for the ping to function, but they are correct now and do not need to be changed.

The subnet mask of the S1 interface on R2 does not need to be changed to 255.255.255.0. The mask needs to match that of R1, which is 255.255.255.252.

Objective:

Infrastructure Services

Sub-Objective:

Troubleshoot client connectivity issues involving DNS

References:

Licensed to Berend Post berend.post@it-university.nl

Question 383

Which Cisco Internetwork Operating System (IOS) command is used to encrypt passwords on Cisco routers?

- ☐ password secure
- ☐ service encryption-password
- ☒ service password-encryption
- ☐ enable password

Explanation:

Explanation:

The service password-encryption command is used to encrypt passwords on Cisco routers. It is used to encrypt all passwords configured on the router, both current and future. This means all passwords in the plain text configuration file will be encrypted. This command is issued in global configuration mode. The syntax of the command is as follows:

Router(config)# service password-encryption

This command does not have any parameters.

Once executed any password in the configuration file will appear similar to what is shown below when the running or startup configuration files are viewed:

R1#show run

<output omitted>

line console 0

password 7 09-4f60C0B1C1B

login

<output omitted>

The password secure and service encryption-password commands are incorrect because they are not valid Cisco IOS commands.

The enable password command is used to set the privileged EXEC mode password, and does not encrypt the password by default.

Objective:

Licensed to Berend Post berend.post@it-university.nl

Infrastructure Security

Sub-Objective:

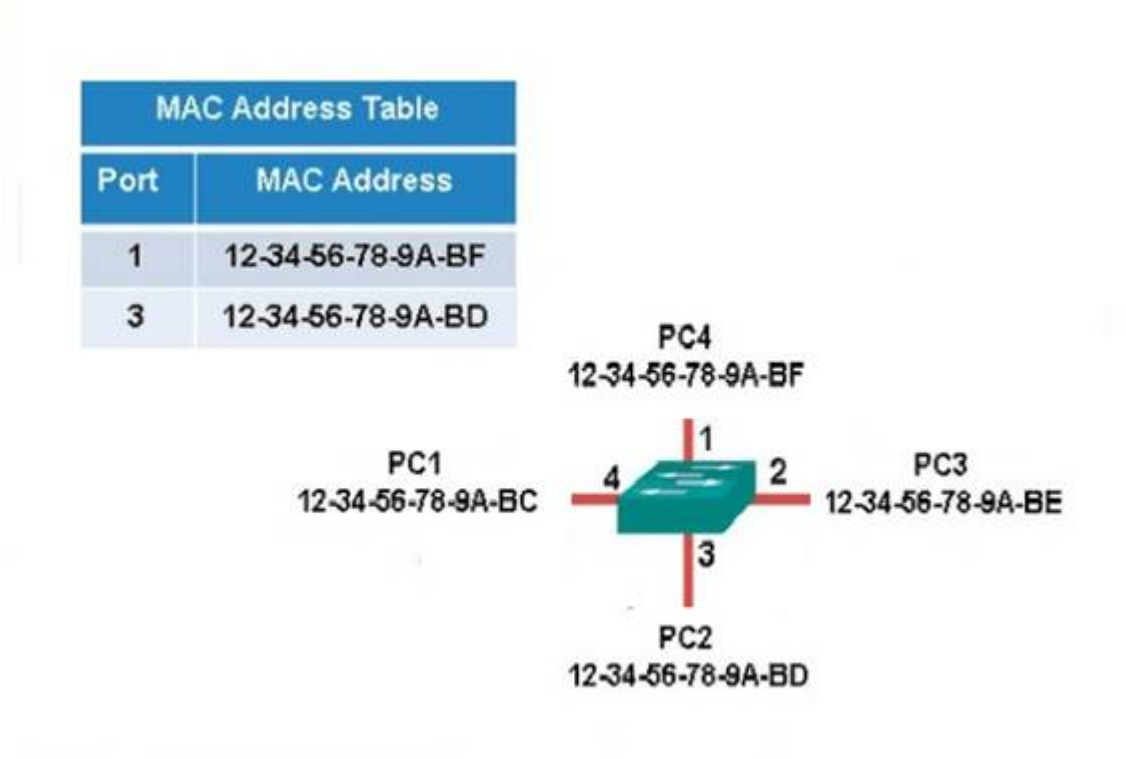
Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Cisco IOS Security Configuration Guide, Release 12.4 > Part 7: Secure Infrastructure > Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Question 384

The exhibit displays the MAC address table of a switch in your network, along with the location of each device connected to the switch.



Which of the following frames will cause the switch to add a new MAC address to its table and forward the frame to all ports when the frame is received?

- ☒ source MAC: 12-34-56-78-9A-BC, destination MAC: ff-ff-ff-ff-ff-ff
- ☐ source MAC: ff-ff-ff-ff-ff, destination MAC: 12-34-56-78-9A-BC
- ☐ source MAC: 12-34-56-78-9A-BF, destination MAC: 12-34-56-78-9A-BC
- ☐ source MAC: 12-34-56-78-9A-BC, destination MAC: 12-34-56-78-9A-BF

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The only frame that will be handled in the specified way is the one with a source MAC of 12-34-56-78-9A-BC and a destination MAC of ff-ff-ff-ff-ff-ff. Since the source address 12-34-56-78-9A-BC is not already in the MAC table, the switch will add it. It will forward the frame to all ports because the destination is the broadcast MAC address of ff-ff-ff-ff-ff-ff.

A frame with a source MAC of ff-ff-ff-ff-ff-ff and a destination MAC of 12-34-56-78-9A-BC is an impossible combination. That would mean that the frame is coming from all devices, which is not possible.

The frame with a source MAC of 12-34-56-78-9A-BF and a destination MAC of 12-34-56-78-9A-BC would be sent to all ports because the destination MAC address is not in the MAC address table. However, the switch would not add a new MAC address to the table because the source address is already in the table.

The frame with a source MAC of 12-34-56-78-9A-BC and a destination MAC of 12-34-56-78-9A-BF would not be forwarded to all ports because the destination MAC address is in the table. The switch would add a new MAC address to the table because the source MAC address is not currently in the MAC address table.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Interpret Ethernet frame format

References:

Cisco Press > Articles > Cisco Certification > CCNA Routing and Switching > Basic Data Transmission in Networks: MAC Tables and ARP Tables

How do Switches Work?

Question 385

At which layer in the Open Systems Interconnection (OSI) model does flow control generally operate?

- ☐ the Network layer
- ☒ the Transport layer
- ☐ the Physical layer
- ☐ the Session layer

Explanation:

Licensed to Berend Post berend.post@it-university.nl

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:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics > Internet Protocols > TCP

Question 386

What will an EIGRP router do if the successor route fails and there is no feasible successor?

- ☐ EIGRP will mark the route as passive until a new successor route is determined.
- ☐ EIGRP will redistribute routes into RIP or OSPF.
- ☒ EIGRP will query neighboring routers until a new successor route is determined.
- ☐ EIGRP will forward traffic to the neighbor with the lowest administrative distance.

Explanation:

Explanation:

Feasible successors are backup routes for the successor (active) route to a remote network. If a successor route fails, and a feasible successor is available, the feasible successor will immediately

Licensed to Berend Post berend.post@it-university.nl

become the successor and be installed in the routing table. This provides EIGRP with virtually instantaneous convergence. If no feasible successor is available, then the router must send out query packets to neighboring EIGRP routers to find an alternate path to the remote network.

EIGRP routes are marked as active when the network is converging. Passive routes are stable, converged routes.

EIGRP will not redistribute routes into RIP or OSPF. Redistribution allows information learned from one routing protocol to be converted into routes for injection into the autonomous system of another routing protocol. This allows networks learned via EIGRP, for example, to be visible and reachable from hosts in a RIP routing domain. Redistribution has nothing to do with EIGRP convergence or with the determination of a new successor route.

Administrative distance is used to determine which source of routing information is considered more trustworthy when multiple routing protocols have been implemented. Administrative distance has no effect on EIGRP convergence or the determination of a new successor route.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

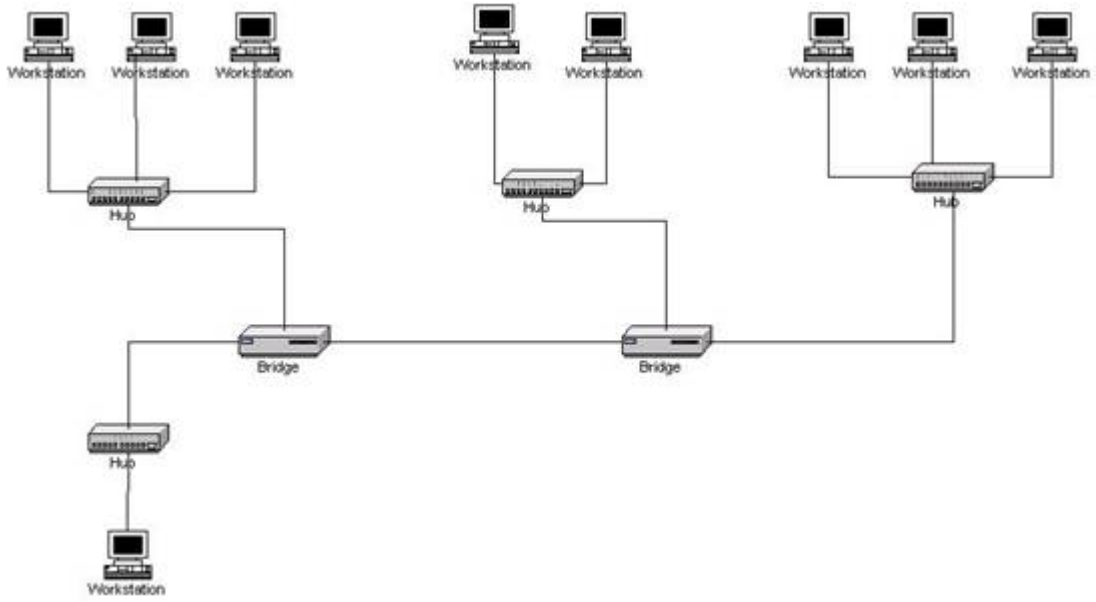
References:

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > Enhanced Interior Gateway Routing Protocol > Document ID: 16406 > Feasible Distance, Reported Distance, and Feasible Successor

Licensed to Berend Post berend.post@it-university.nl

Question 387

How many collision domains are in a LAN with four hubs and two bridges that are connected directly to each other, as shown in the following figure? (Click the Exhibit(s) button.)



- ☐ four
- ☒ five
- ☐ six
- ☐ fourteen

Explanation:

Explanation:

A bridge segments the LAN into separate collision domains. The figure in this scenario has five segments created between these two bridges. Therefore, there will be five collision domains (segments) on the LAN if the two bridges are directly connected as shown in the exhibit. Hubs do not create LAN segments; they act as port aggregators and signal amplifiers.

It is also worth noting that with no router in the diagram, the entire network is a single broadcast domain. If a router were present, each of its interfaces could host a different subnet and each of those same interfaces would be a separate broadcast domain.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Licensed to Berend Post berend.post@it-university.nl

Internetwork Design Guide -- Designing Switched LAN Internetworks > Comparison of LAN Switches and Routers

Question 388

Which Cisco IOS command configures the clock rate to 64,000 bits per second on an interface?

- ☐ clock-rate 64000
- ☐ clock rate 64k
- ☒ clock rate 64000
- ☐ clockrate 64000

Explanation:

Explanation:

The clock rate 64000 command would configure the clock rate to 64,000 bits per second on an interface. The clock rate command is used to configure the clock rate for hardware connections on serial interfaces. These interfaces can be network interface modules (NIMs) and interface processors. The syntax of this command is clock rate bps.

A serial connection between two routers that are connected with a v.35 serial cable requires a clock rate on the Data Communications Equipment (DCE) end of the cable, but not on the Data Terminal Equipment (DTE) end. When the router is connected to a CSU/DSU for connection to the outside world, the DCE end will be the CSU/DSU. In a lab environment or any situation where you have two routers connected with this type of serial cable, a clock rate must be set on the DCE end of the cable.

When troubleshooting a connection of this type between routers, the state of the clock rate (set or unset) can be determined by running the show controllers command on the DCE end. The output will display as follows if the clock rate is NOT set:

Router#show controllers s0/0

Interface Serial0/0

Hardware is PowerQUICC MPC860

DTE V.35 clocks stopped

More output omitted

Notice the DTE V.35 clocks stopped line, which indicates no clock rate is set. Another clue that there is a Layer 2 problem is the output of the show ip interface S0/0 command, executed on the same interface below:

Licensed to Berend Post berend.post@it-university.nl

Router# show ip interface s0/0

Serial0/0 is up, line protocol is down

Internet address is 192.168.1.2/24

Broadcast address is 255.255.255.255

Notice the Serial0/0 is up, line protocol is down line. Serial0/0 is up indicates that the physical connection is good, but line protocol is down indicates a problem with Layer 2 . If you were troubleshooting from the bottom layer to the top, you would now check Layer 2, which would be the clock rate.

If you want to change a DCE interface to a DTE device, you should use the no clock rate command.

All the other options are incorrect because these commands are syntactically incorrect.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Question 389

Which of the following commands sets the local router to serve as an authoritative time source?

- ☐ ntp server
- ☒ ntp master
- ☐ ntp authenticate
- ☐ ntp peer

Explanation:

Explanation:

The ntp master command sets the local router to serve as an authoritative time source.

The ntp server command is used to specify an external time source that the local router should use as its time source.

Licensed to Berend Post berend.post@it-university.nl

The ntp authenticate command is used to enable the authentication of time source to which the local router has been configured to use. It is the first step in a process that must also include the specification of a hashing algorithm and a key, both of which must match on the time source.

The ntp peer command is used to configure the local router to synchronize a peer or to be synchronized by a peer. It does not make the local router authoritative as a time source like the ntp master command.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify NTP operating in a client/server mode

References:

Cisco > Support > Cisco IOS Basic System Management Command Reference > ntp master

Question 390

You are planning the configuration of an IPsec-protected connection between two routers. You are concerned only with the integrity of the data that passes between the routers. You are less concerned with the confidentiality of the data, and you would like to minimize the effect of IPsec on the data throughput.

Which protocol option should you choose?

- ☒ Authentication Header (AH) in tunnel mode
- ☐ Authentication Header (AH) in transport mode
- ☐ Encapsulating Security Payload (ESP) in tunnel mode
- ☐ Encapsulating Security Payload (ESP) in transport mode

Explanation:

Explanation:

You should choose Authentication Header (AH) in tunnel mode to meet the scenario requirements. Two protocols can be used to build tunnels and protect data traveling across the tunnel:

Authentication Header (AH) uses protocol 51.

ESP uses protocol 50.

AH is defined in Request for Comments (RFC) 1826 and 2402. AH does not perform data encryption, and therefore information is passed as clear text. The purpose of AH is to provide data integrity and

Licensed to Berend Post berend.post@it-university.nl

authentication, and optionally to provide anti-reply service. It ensures that a packet that crosses the tunnel is the same packet that left the peer device and no changes have been made. It uses a keyed hash to accomplish this.

ESP is defined in RFC 2406. ESP can provide data integrity and authentication, but its primary purpose is to encrypt data crossing the tunnel. On Cisco devices, ESP supports encryption using Advanced Encryption Standard (AES), Data Encryption Standard (DES), or Triple DES (3DES). Tunnel mode is used between Virtual Private Network (VPN) gateways such as routers, firewalls, and VPN concentrators.

You would not choose Authentication Header (AH) in transport mode. Transport mode is used between end stations or between an end station and a VPN gateway.

You would not choose Encapsulating Security Payload (ESP) in tunnel mode or transport mode. Using ESP will slow the connection because of the encryption and decryption process that will occur with each packet.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco > Articles > Network Technology > General Networking > IPsec Overview Part Two: Modes and Transforms

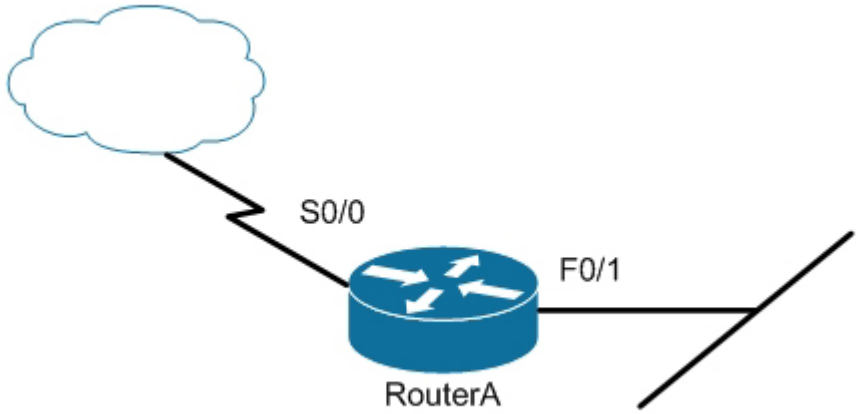
Cisco > The Internet Protocol Journal > The Internet Protocol Journal - Volume 3, No. 1, March 2000 > IP Security

CCNA ICND2 Official Exam Certification Guide (Cisco Press, ISBN 1-58720-181-X), Chapter 15: Virtual Private Networks, pp. 536-537.

Licensed to Berend Post berend.post@it-university.nl

Question 391

Users on the LAN are unable to access the Internet. How would you correct the immediate problem?



Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol
FastEthernet 0/0 unassigned YES unset down down
FastEthernet 0/1 172.16.1.254 YES NVRAM up up
Serial0/0 200.16.4.25 YES NVRAM administratively down down
Serial0/1 unassigned YES unset down down

- ☐ Configure a bandwidth on the serial interface.
- ☒ Perform a no shutdown command on the serial interface.
- ☐ Configure a private IP address on the Fastethernet0/0 LAN interface.
- ☐ Change the IP address on the serial interface.

Explanation:

Explanation:

The output indicates that the serial interface leading to the Internet is administratively down. All router interfaces are disabled by default due to the presence of a shutdown command in the running configuration. The no shutdown command removes this configuration, and the interface becomes active. The command sequence is:

Router(config)# interface serial0/0

Router(config-if)# no shutdown

Although it was not the problem in the scenario, the S0/0 interface could also cause an error if it is configured as shown in this output:

Interface IP-Address OK? Method Status Protocol

Licensed to Berend Post berend.post@it-university.nl

Serial0/0 200.16.4.25 YES NVRAM up down

In this example, the S0/0 interface has been enabled, and while there is Layer 1 connectivity (the Status column), Layer 2 is not functioning (the Protocol column). There are two possible reasons for this result:

Interface S0/0 is not receiving a clock signal from the CSU/DSU (if one is present).

The encapsulation type configured on S0/0 does not match the type configured on the other end of the link (if the other end is a router).

Configuring a bandwidth on the serial interface is incorrect because the output indicates the interface is administratively down, which does not pertain to bandwidth.

Configuring a private IP address on the Fastethernet0/0 LAN interface is incorrect because the output indicates the problem is with the disabled serial interface.

The IP address on the serial interface may or may not be valid, but it is not the immediate cause of the connectivity problem. The serial interface is disabled.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Cisco > Support > Administrative Commands > shutdown

Licensed to Berend Post berend.post@it-university.nl

Question 392

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?

- ☐ FEC0:0:0:1::1/64
- ☒ FE80::260:3EFF:FE11:6770/10
- ☐ 2001:0410:0:1:0:0:0:1/64
- ☐ 2002:500E:2301:1:20D:BDFF:FE99:F559/64

Explanation:

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

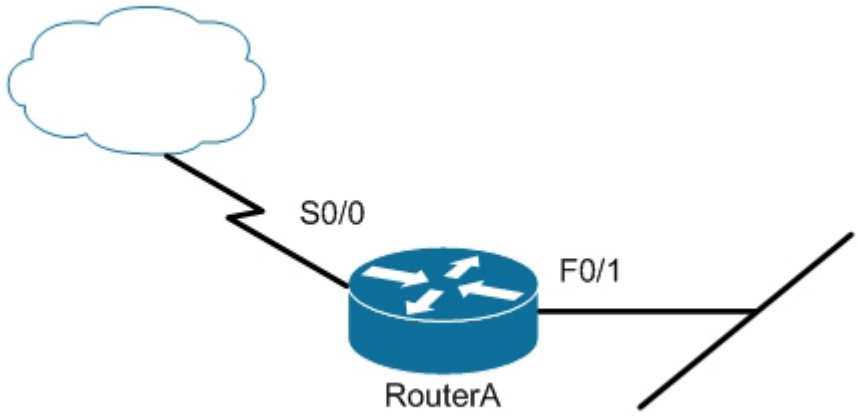
References:

Cisco > Understanding IPv6 Link Local Address

Licensed to Berend Post berend.post@it-university.nl

Question 393

Users on the LAN are unable to access the Internet. How would you correct the immediate problem?



Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol
FastEthernet 0/0 unassigned YES unset down down
FastEthernet 0/1 172.16.1.254 YES NVRAM up up
Serial0/0 200.16.4.25 YES NVRAM administratively down down
Serial0/1 unassigned YES unset down down

- ☐ Configure a bandwidth on the serial interface.
- ☒ Perform a no shutdown command on the serial interface.
- ☐ Configure a private IP address on the Fastethernet0/0 LAN interface.
- ☐ Change the IP address on the serial interface.

Explanation:

Explanation:

The output indicates that the serial interface leading to the Internet is administratively down. All router interfaces are disabled by default due to the presence of a shutdown command in the running configuration. The no shutdown command removes this configuration, and the interface becomes active. The command sequence is:

Router(config)# interface serial0/0

Router(config-if)# no shutdown

Although it was not the problem in the scenario, the S0/0 interface could also cause an error if it is configured as shown in this output:

Licensed to Berend Post berend.post@it-university.nl

Interface IP-Address OK? Method Status Protocol

Serial0/0 200.16.4.25 YES NVRAM up down

In this example, the S0/0 interface has been enabled, and while there is Layer 1 connectivity (the Status column), Layer 2 is not functioning (the Protocol column). There are two possible reasons for this result:

Interface S0/0 is not receiving a clock signal from the CSU/DSU (if one is present).

The encapsulation type configured on S0/0 does not match the type configured on the other end of the link (if the other end is a router).

Configuring a bandwidth on the serial interface is incorrect because the output indicates the interface is administratively down, which does not pertain to bandwidth.

Configuring a private IP address on the Fastethernet0/0 LAN interface is incorrect because the output indicates the problem is with the disabled serial interface.

The IP address on the serial interface may or may not be valid, but it is not the immediate cause of the connectivity problem. The serial interface is disabled.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Cisco > Support > Administrative Commands > shutdown

Licensed to Berend Post berend.post@it-university.nl

Question 394

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?

- ☐ show ip arp
- ☐ debug ip rip
- ☒ show ip protocols
- ☐ show ip routing process
- ☐ show arp
- ☐ show interfaces

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

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.

Licensed to Berend Post berend.post@it-university.nl

Note: Before running any debug command you should execute the show processes command and verify that the CPU utilization on the router is low enough to handle the effects of running the debug command.

The show ip routing process command is incorrect because it is not a valid Cisco IOS command.

The show arp command is used to identify the IP address to MAC address mappings the router has leaned through the ARP broadcast process. It is helpful when you have identified errors associated with a MAC address and you need to learn the IP address or vice versa. Sample output is below.

router# show arp

Protocol Address Age (min) Hardware Addr Type Interface

Internet 10.0.0.3 0 0004.dd0c.ffcb ARPA Ethernet01

Internet 10.0.0.1 - 0004.dd0c.ff86 ARPA Ethernet0

The difference between the show arp command and the show ip arp command is that show arp will also include mappings learned through non-IP protocols such as when inverse ARP is used to learn and map DLCIs to IP addresses.

The show interface command can also be used to identify IP addresses from MAC addresses and vice versa, but also indicates the state of the interface; IP addresses MTU and much more about each interface. Sample output is below.

router# show interfaces

Ethernet 0 is up, line protocol is up

Hardware is MCI Ethernet, address is 0000.0c00.750c(bia 0000.0c00.750c)

Internet address is 10.108.28.8, subnet mask is 255.255.255.0

MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Cisco IOS IP Routing Protocols Command Reference > IP Routing Protocol-Independent Commands: S through T > show ip protocols

Question 395

Which command(s) will enable you to configure only serial interface 0 on a Cisco router?

- ☐ router>interface serial 0
- ☐ router#interface serial 0
- ☒ router(config)#interface serial 0
- ☒ router(config-if)#interface serial 0

Explanation:

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)

Licensed to Berend Post berend.post@it-university.nl

Router(config-if)# no shutdown (enables or "turns on" the interface)

Router(config-if)# exit (exits global configuration mode)

Router(config)# exit (exits privileged mode)

Router# copy running-config startup config (copies the changes to the configuration file on the router)

Alternately, you could enter interface configuration mode for one interface while still in configuration mode for another interface, as shown below. After entering the interface serial 1 command, you will be editing serial 1 instead of serial 0.

Router(config)# interface serial 0

Router(config)#

Router(config)# interface serial 1

You should not use the command router> interface serial 0. User EXEC mode, as indicated by the prompt router>, provides limited access to a router and is the initial mode you see after authenticating to the router. The subcommand interface serial 0 is not functional before you proceed to global configuration mode and interface configuration mode for a specific interface.

You should not use the command router# interface serial 0. Privileged mode (as indicated by the prompt router#) must be traversed to get to global configuration mode before you can execute the subcommand interface serial 0. This subcommand is not functional while you are still in privileged mode.

Objective:

Infrastructure Management

Sub-Objective:

Use Cisco IOS tools to troubleshoot and resolve problems

References:

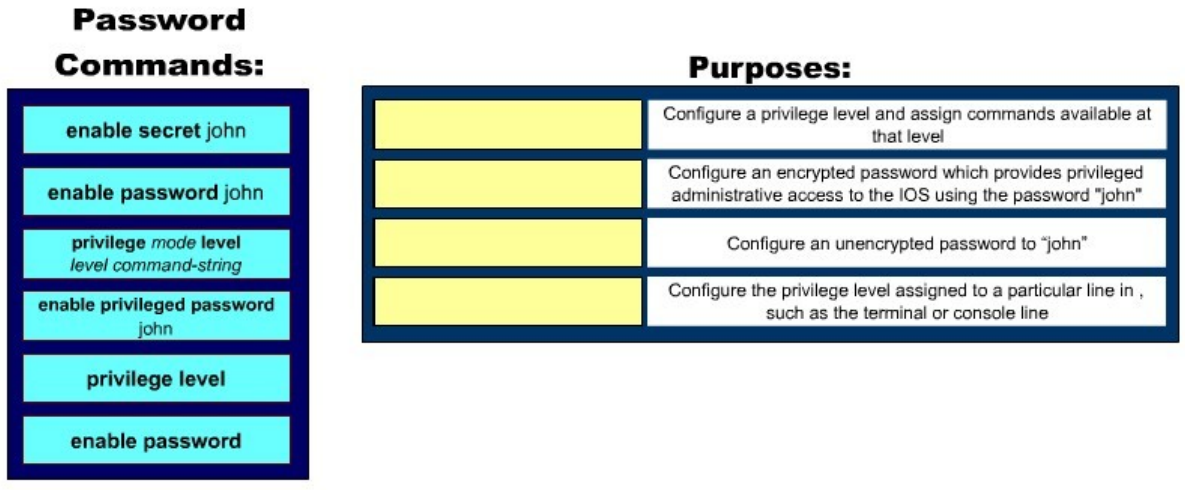
Cisco > Cisco 1600 Series Software Configuration Guide > Cisco IOS Software Basic Skills

Licensed to Berend Post berend.post@it-university.nl

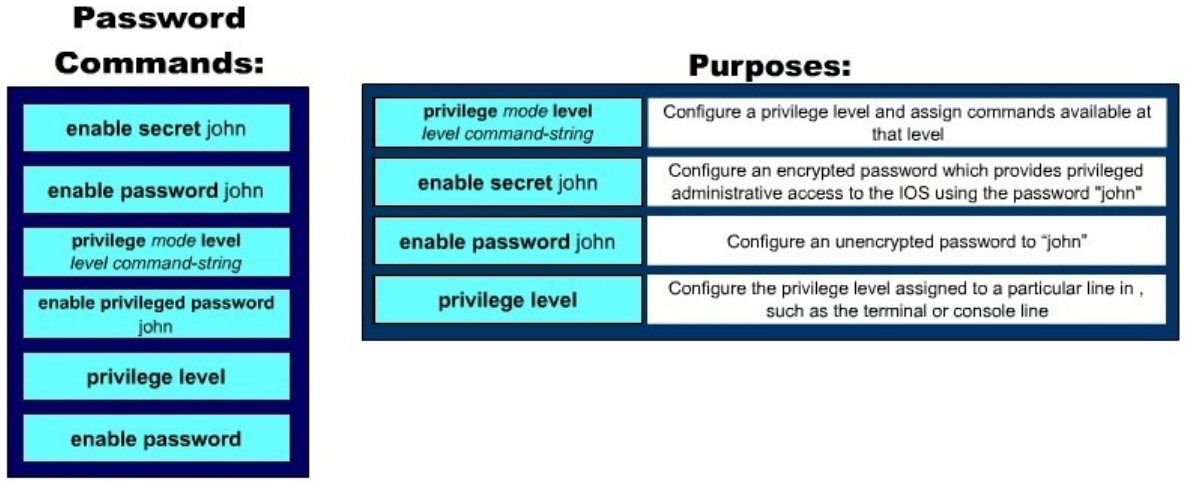
Question 396

DRAG DROP

Click and drag the command(s) used to configure passwords on a Cisco router to their appropriate purposes. (Not all options will be used.)



Solution:



Explanation:

Explanation:

Following are the commands along with their descriptions:

enable secret john: The enable secret command is used to configure an encrypted password, which provides privileged administrative access to the IOS using the password "John". It is always advisable to configure an enable secret password. If an enable secret password is not configured and a console TTY password is configured, then a remote user can gain privileged administrative access from a remote VTY session which poses a risk to the network security.

enable password john: The enable password command is used to configure an unencrypted password.

Licensed to Berend Post berend.post@it-university.nl

To set a user mode password, which is one that you are prompted for when you connect to the router rather than when you try to execute the enable command, enter the line at which you want it effective (either line console 0, line aux 0, or line vty 0 4) and then password <password>. An example of setting the user mode password for both the console and the telnet connections are shown below:

Router(config)#Line console 0

Router(config-line)#login

Router(config-line)#password cisco

Router(config)#Line vty 0 4

Router(config-line)#login

Router(config-line)#password cisco

Also be aware that as executed above the password will not be encrypted without the execution of the service password-encryption command prior to creating the passwords.

privilege level: This command is used to configure the privilege level assigned to a particular line in, such as the terminal or console line

privilege mode level level command-string: This command would be used to configure a particular privilege level and assign commands available at that level.

The other options offered are not valid commands.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

References:

Cisco > Tech Notes > Improving Security on Cisco Routers > Document ID: 13608 > Password Management

Licensed to Berend Post berend.post@it-university.nl

Question 397

Which of the following topologies is used in Wide Area Networks (WANs)?

- ☐ FDDI
- ☐ CDDI
- ☒ SONET
- ☐ Token Ring

Explanation:

Explanation:

Synchronous Optical NETwork (SONET) is the standard topology for fiber optic networks. Developed in 1980s, SONET can transmit data at rates of up to 2.5 gigabits per second (Gbps).

All other options are incorrect because they are LAN topologies, not WAN topologies.

Fiber Distributed Data Interface (FDDI) specifies a 100-Mbps dual-ring fiber optics-based token-passing LAN. FDDI is typically implemented for high-speed LAN backbones because of its support for high bandwidth.

Copper Distributed Data Interface (CDDI) is copper version of FDDI. They differ only in that FDDI can span longer distances than CDDI due to the attenuation characteristics of copper wiring.

Token Ring/IEEE 802.5 LAN technology was developed by IBM in 1970. Token-ring LAN technology is based on token-passing, in which a small frame, called a token, is passed around the network. Possession of the token grants the node the right to transmit data. Once the data is transmitted, the station passes the token to the next end station.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast network topologies

References:

Cisco>Home>Cisco Documentation > Internetworking Technology Handbook>WAN Technologies

Licensed to Berend Post berend.post@it-university.nl

Question 398

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?

- ☐ The relevant switch ports will be green.
- ☐ The relevant switch ports will be amber.
- ☒ The relevant switch ports will be neither green nor amber.
- ☐ The relevant switch ports will be green and flashing.

Explanation:

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)

Licensed to Berend Post berend.post@it-university.nl

References:

Question 399

Which of the following cables would be used to connect a router to a switch?

- ☐ v.35
- ☐ crossover
- ☐ rollover
- ☒ straight-through

Explanation:

Explanation:

A straight-through cable would be used. When connecting "unlike" devices, such as a switch to a router, a straight-through cable is used. This is a cable where the wires are in the same sequence at both ends of the cable.

NOTE: The one exception to this general rule of connecting unlike devices with a straight-through cable is when a computer NIC is connected to an Ethernet port on a router. In that case, a crossover cable is used.

A v.35 cable is used to connect serial connections between routers. This cable has a male DB-60 connector on the Cisco end and a male Winchester connector on the network end. It comes in two types: DCE and DTE. It is often used to simulate a WAN connection in lab environments. In that case, the DCE end acts as the CSU/DSU and is the end where the clock rate is set. A CSU/DSU (Channel Service Unit/Data Service Unit) is a device that connects the router to the T1 or T3 line.

A crossover cable has two wires reversed and is used to connect "like" devices, such as a switch to a switch. It is also used when a computer NIC is connected to an Ethernet port on a router.

A rollover cable is used to connect to the console port of a router to configure the router. It is also called a console cable.

The diagram below illustrates the correct usage of each of the cable types shown using the following legend:

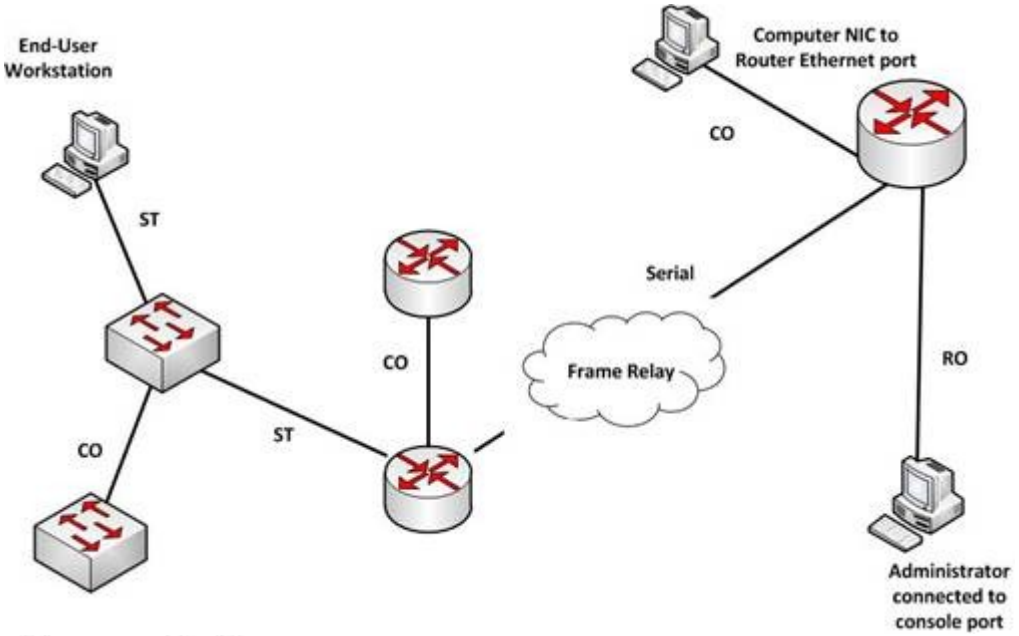
SO Ethernet Straight through Cable

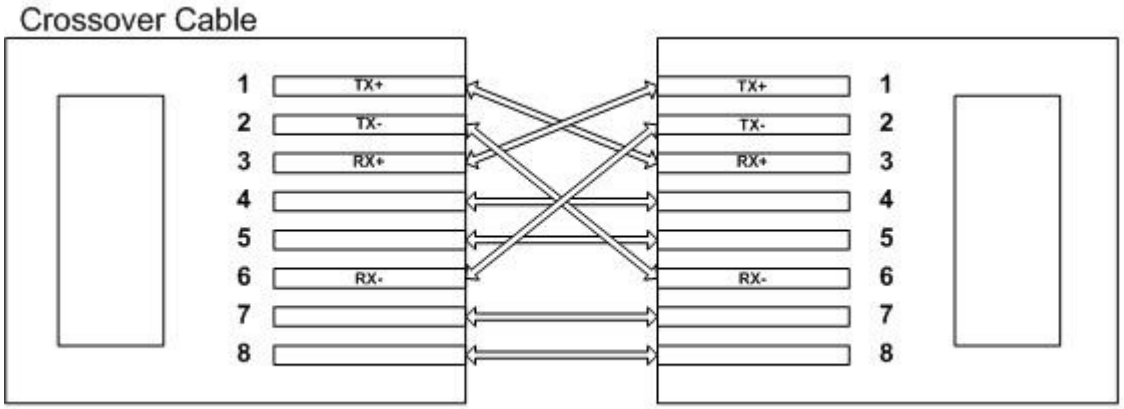
CO Ethernet Crossover Cable

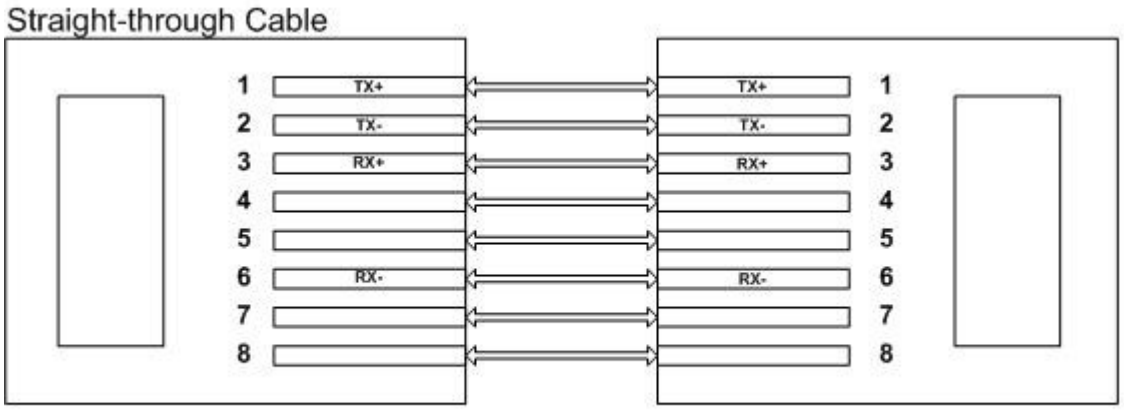
Serial Serial cable

RO Rollover cable

Licensed to Berend Post berend.post@it-university.nl







RX = Receive, TX = Transmit

Objective:

Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Product Support > Routers > Cisco 1000 Series Routers > 5-in-1 V.35 Assembly and Pinouts > Document ID: 46803

Cisco > Tech Notes > Cabling Guide for Console and AUX Ports > Document ID: 12223

Question 400

Which Cisco Internetwork Operating System (IOS) command is used to view the VLAN Trunking Protocol (VTP) statistics information?

- ☐ show vtp status
- ☐ show vtp domain
- ☐ show vtp statistics
- ☒ show vtp counters

Explanation:

Explanation:

The show vtp counters command is used to view VTP statistics information. The syntax of the command is as follows:

show vtp {counters | status}

The parameters used in the command are counters, which specifies VTP statistics information, and status, which specifies VTP domain status information.

The following is the output of the show vtp counters command:

Licensed to Berend Post berend.post@it-university.nl

```
Router#show vtp counters

VTP statistics:
Summary advertisements received: 7
Subset advertisements received: 6
Request advertisements received: 0
Summary advertisements transmitted: 894
Subset advertisements transmitted: 13
Request advertisements transmitted: 3
Number of config revision errors: 0
Number of config digest errors: 0
Number of V1 summary errors: 0
VTP pruning statistics:

Trunk Join Transmitted Join Received Summary advts received
from on-pruning-capable device
--------------- ---------------- ---------------- --------------------
Fa0/2 43450 42691 6
```

The show vtp status command option is incorrect because this command is used to view VTP domain status information.

The show vtp domain and show vtp statistics commands are invalid options because they are not valid Cisco IOS commands.

Objective:

Routing Fundamentals

Sub-Objective:

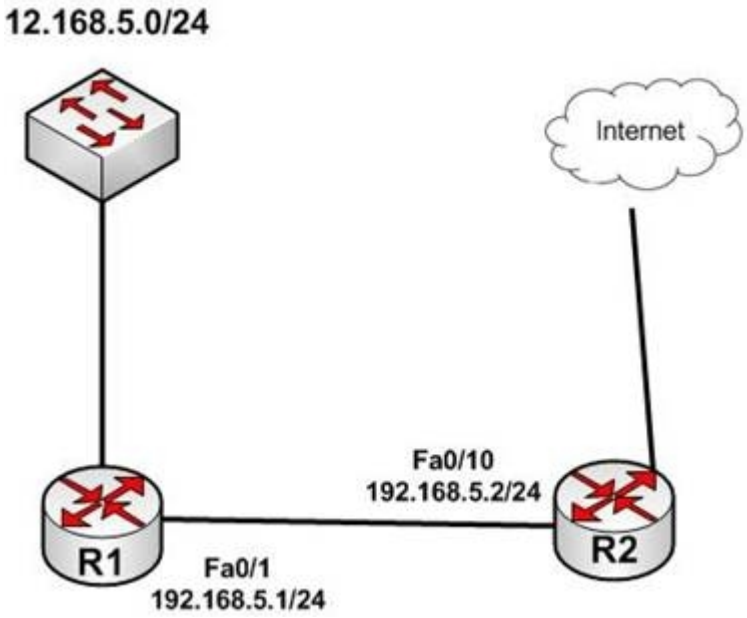
Configure, verify, and troubleshoot inter-VLAN routing

References:

Licensed to Berend Post berend.post@it-university.nl

Question 401

To minimize routing protocol traffic, you have decided to use static routing in the network displayed in the following diagram. You would like to keep the configuration as simple as possible.



Which command(s) are required for all hosts to communicate with one another and the Internet? (Choose all that apply.)

- ☐ R1(config)#ip route 12.168.5.0 255.255.255.0 192.168.5.1
- ☐ R2(config)#ip route 0.0.0.0 255.255.255.0 192.168.5.2
- ☐ R1(config-if)# ip route 12.168.5.0 255.255.255.0 192.168.5.1
- ☐ R2(config-if)# ip route 0.0.0.0 255.255.255.0 192.168.5.2
- ☒ R2(config)#ip route 12.168.5.0 255.255.255.0 192.168.5.1
- ☒ R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.5.2

Explanation:

Explanation:

There must be two routes added to make the network functional. From a conceptual standpoint, the network requires the following two routes:

A static default route on R1 that directs all traffic destined for unknown networks (which would include Internet-bound traffic) to R2

A static route on R2 to direct traffic destined for 12.168.5.0/24 to R1. Without this route R2 will be unable to route return traffic to the 12.168.5.0/245 network even if the default route in the first bullet point has been added.

The commands that would create these routes, respectively, are:

R2(config)#ip route 12.168.5.0 255.255.255.0 192.168.5.1

Licensed to Berend Post berend.post@it-university.nl

R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.5.2

Troubleshooting routing problems should always begin with examining the routing table of the routers involved in the path to the destination. If the routes are static, they will also appear in the output of the show run command. One of the characteristics of a static route is that it will remain in the routing table even if routers on the path to the destination network lose their route to the network. If an advertising router loses its route to a destination network, dynamic routes will be removed from the routing tables of the routers that received that advertisement.

Static routes not only reduce routing update traffic in stub networks such as this one, but they also increase security because only the network administrator may change the routing table. On the other hand, the administrator must also stand ready to manually add new routes if current routes become unavailable. Dynamic routing is designed to make these route changes automatically if alternate routes exist.

The commands R1(config-if)# ip route 12.168.5.0 255.255.255.0 192.168.5.1 and R2(config-if)# ip route 0.0.0.0 255.255.255.0 192.168.5.2 are incorrect because they are executed at an interface prompt, rather than at the global configuration prompt as required.

The command ip route 12.168.5.0 255.255.255.0 192.168.5.1 is the correct command to create a static route to direct traffic destined for 12.168.5.0/24 to R1. However, this command should be executed on R2, not at the R1(config)# prompt.

The command ip route 0.0.0.0 0.0.0.0 192.168.5.2 is the correct command to create a static default route that directs all traffic destined for unknown networks (which would include Internet-bound traffic) to R2. However, this command should be executed on R1 and not at the R2(config)# prompt.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 and IPv6 static routing

References:

Cisco IOS IP Configuration Guide, Release 12.2 > Configuring IP Routing Protocol-Independent Features > Configuring Static Routes

Licensed to Berend Post berend.post@it-university.nl

Question 402

Which command was used to create the following configuration?

```
Router# show ip protocol
Routing Protocol is "eigrp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: eigrp 1
Automatic network summarization is in effect
Routing for Networks:
192.168.1.80/28
192.168.1.128/28
Routing Information Sources:
Gateway Distance Last Update
192.168.1.85 90 0:04:01
Distance: internal 90 external 170
```

- ☐ Router(config-router)# network 192.168.1.0 0.0.0.15
- ☐ Router(config-router)# network 192.168.1.0 255.255.255.0
- ☐ Router(config-router)# network 192.168.1.80
- ☐ Router(config-router)# network 192.168.1.128
- ☒ Router(config-router)# network 192.168.1.0

Explanation:

Explanation:

The network 192.168.1.0 command instructs the router to activate EIGRP on every interface that belongs to the class C network 192.168.1.0. The exhibit indicates that the router is running EIGRP on two subnets of 192.168.1.0 (192.168.1.80/28 and 192.168.1.128/28). Since both of these are subnets of the same class C network number, only the class C address needs to be referenced with a network statement.

All interfaces that will participate in EIGRP must be specified with a network command that specifying the network of which the interface is a member. Failure to do so will result in neighbor relationships not forming. In the example below, Router A and Router B are directly connected, but not forming a neighbor relationship. The network they share is the 192.168.5.0/24 network. The output of the show run command for both routers reveals that Router B does not have EIGRP running on the 192.168.5.0 network.

```
RouterA#show run                    Router B#show run
<output omitted>            <output omitted>
router eigrp 36                       router eigrp 36
network 192.168.5.0                 network 10.0.0.0
```

The network 192.168.1.0 0.0.0.15 command is incorrect because only the class C network number (192.168.1.0) needs to be referenced to enable EIGRP on all subnets. It is actually valid to include an inverse mask with EIGRP network statements, but it is unnecessary in this case, and the network/mask provided does not match either of the routed networks.

Licensed to Berend Post berend.post@it-university.nl

The network 192.168.1.0 255.255.255.0 command is incorrect because the mask is unnecessary in this case, and if masks are included, they must be expressed inversely (0.0.0.255).

It is unnecessary to configure two network commands in this example, as both networks are subnets of the same class C network (192.168.1.0), and a single network command can enable EIGRP on both. Additionally, if specific subnets are referenced in network commands, it is necessary to include an inverse mask after them, or EIGRP will automatically summarize the command to the classful boundary.

Objective:

Routing Fundamentals

Sub-Objective:

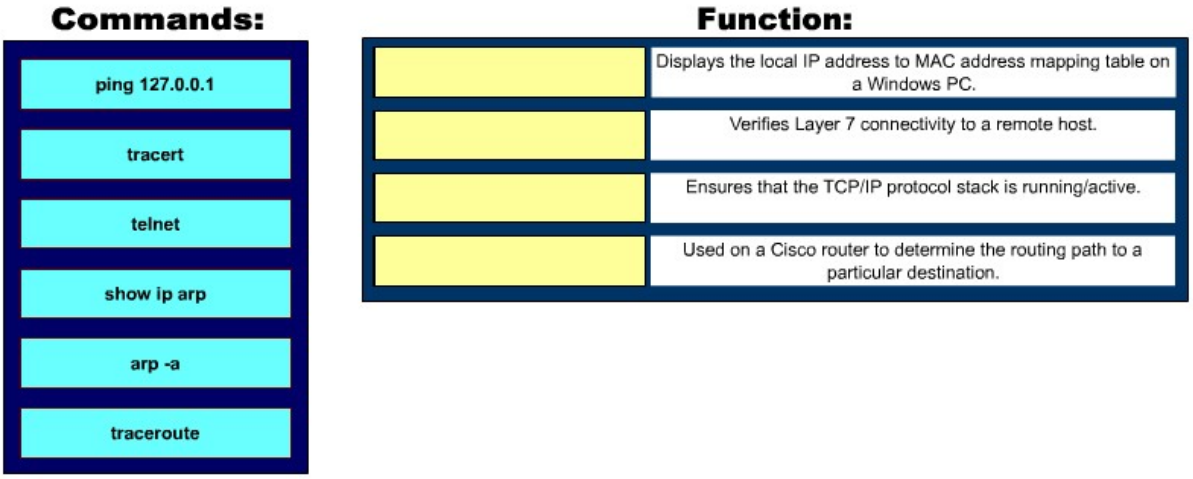
Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T > Part 3: EIGRP > Configuring EIGR

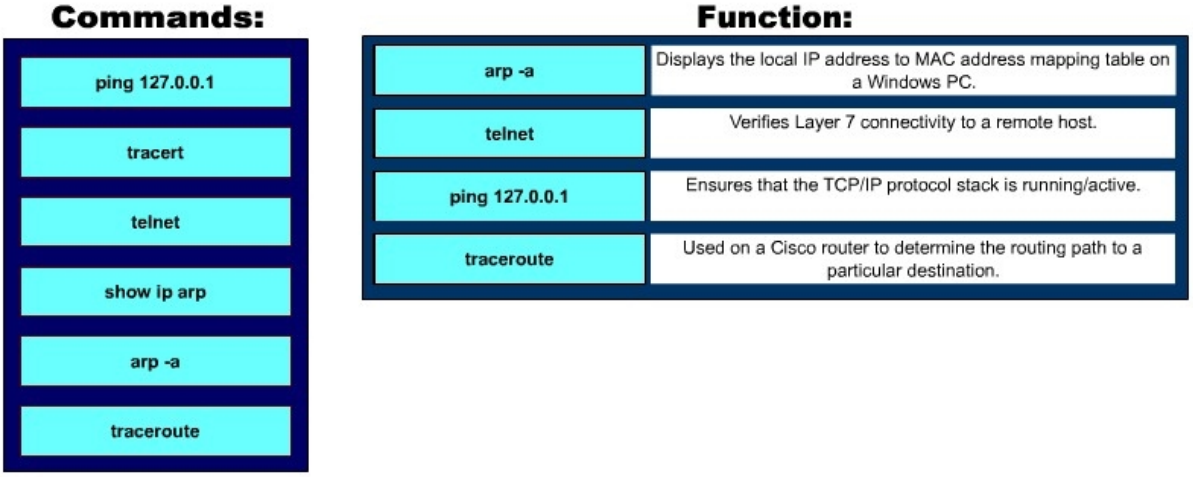
Question 403

DRAG DROP
Click and drag the command line tools used to troubleshoot the network problems on the left to their associated functions on the right. Not all commands may be used.



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

Explanation:

The following commands can be used to troubleshoot network connectivity problems:

ping 127.0.0.1: This command will attempt to contact the local TCP/IP protocol stack. The 127.0.0.1 address is the reserved loopback IP address, which allows applications to communicate with the local system without using an actual IP address assigned to an interface, such as a workstations Ethernet port. Thus, this command allows you to ping yourself?, and if successful, only verifies that TCP/IP is running locally. It does not confirm that the system can communicate with any other host on the network.

telnet: Telnet is a network application used to establish a remote terminal connection to a host, such as logging in remotely to a Cisco router or switch via TCP/IP. Since network applications reside on the OSI Application Layer (Layer 7), a successful Telnet connection to a remote has confirms that there is network connectivity through Layer 7.

arp? a: This command is used to display the local IP address to MAC address mappings on a Windows PC.

traceroute: This command is used on a Cisco router or switch to verify, or trace, the path that IP packets will take towards a particular destination.

tracert: This command is used on a Windows PC to verify, or trace, the path that IP packets will take towards a particular destination.

show ip arp: This command is used to display the local IP address to MAC address mappings on a Cisco router or switch.

Objective:

Routing Fundamentals

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Support > Troubleshooting Tools

Cisco > Articles > Cisco Certification > CCNP > Shooting Trouble with IP

Question 404

A switch is powered up, and the system LED is amber.

Which of the following describes this situation?

- ☒ The switch is malfunctioning.
- ☐ Utilization level is high.
- ☐ The switch is performing normally.
- ☐ There is a security violation on a switch port.

Explanation:

Explanation:

The system LED indicates the overall health of the switch. The LED should turn solid green after a successful Power On Self Test (POST). An amber system LED indicates that there is a system-wide failure in the switch.

High utilization will not cause the system LED to turn amber.

An amber system LED indicates a general switch malfunction. It does not indicate that the switch is performing normally.

Port security violations will not cause the system LED to be amber. The system LED is used to identify the overall health of the switch.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Catalyst 2960 Switch Hardware Installation Guide > LEDs

Question 405

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?

- ☒ Stateless DHCPv6
- ☐ Stateful DHCPv6
- ☐ DHCPv6-PD
- ☐ Stateless autoconfiguration

Explanation:

Explanation:

Stateless DHCPv6 uses a combination of processes to assign a configuration to an IPv6 interface. It uses Stateless Address Autoconfiguration (SAAC), a process native to IPv6, to assign an IPv6 address to the interface. It uses DHCPv6 to assign other parameters, such as the DNS server and NTP server.

In stateful DHCPv6, the interface will receive the IPv6 address and all other parameters from the DHCP server.

In DHCPv6 Prefix Designation (DHCPv6-PD), the device is assigned a set of IPv6 "subnets." This assignment will consist of a set of IPv6 addresses in the same subnet (such as the address 2001:db8::/60) that the device can dynamically allocate to its interfaces.

Objective:

Network Fundamentals

Sub-Objective:

Configure and verify IPv6 Stateless Address Auto Configuration

References:

Cisco > Support > IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3S > Chapter: IPv6 Access Services: Stateless DHCPv6

Licensed to Berend Post berend.post@it-university.nl

Question 406

Which cable can suffer attenuation if it is bent beyond the minimum bend radius?

- ☐ UTP
- ☐ STP
- ☐ Co-axial
- ☒ Fiber optic

Explanation:

Explanation:

Fiber-optic cables can suffer attenuation if they are bent beyond the minimum bend radius. Fiber-optic cables work on the principle of total internal reflection. The fiber optic cable uses a laser and glass tubes with refractive internal coating to achieve total internal reflection. If a light ray travelling in the tube is bent at a certain angle, the light ray will be reflected inside the medium instead of passing through the medium. If the fiber optic cables are bent beyond the minimum bend radius, the signal will be lost and the cable will suffer attenuation. Fiber cables are expensive and are typically used for outdoor campus backbone. However, as the fiber cables use light to carry signals, they are not affected by the electro-magnetic interference (EMI) generated by electric cables.

Another advantage of fiber optic cabling is its applicability to situations where electrical issues may exist in the environment. Even in situations where the length of the cable run is well within the attenuation limits of STP (for example 55 meters), voltage differences between buildings can cause issues. That is a problem that can be solved by using fiber on the run, which is not impacted by electrical issue.

All other cables typically use copper to carry low voltage signals and are not affected by normal bending. However, even copper cables may suffer some signal loss if there are bends in the cable.

Objective:

Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

Cisco > Articles > Network Technology > General Networking > Fiber-Optic Technologies

Licensed to Berend Post berend.post@it-university.nl

Question 407

Which switch port will be in a blocking state? (Click the Exhibit(s) button to view the switch port diagram.)



- ☐ SwitchA Fa0/1
- ☐ SwitchA Fa0/2
- ☐ SwitchB Fa0/1
- ☒ SwitchB Fa0/2

Explanation:

Explanation:

SwitchB will be forwarding on F0/1, and blocking on F0/2.

SwitchA will become the STP root bridge due to its lower MAC address. All ports on the root bridge will become designated ports in a forwarding state. SwitchB has redundant connectivity to the root bridge, and must block one of its interfaces to prevent a switching loop. STP will use its operations to determine which of the redundant interfaces on SwitchB to block to prevent a switching loop

Both interfaces are the same speed (FastEthernet), and thus their cost to the root is the same.

Finally, the interface with the lowest number will become the forwarding port. F0/1 has a lower port number than F0/2, so F0/1 becomes a forwarding port, and F0/2 becomes a blocking port.

Note: Unlike STP, Rapid Spanning Tree Protocol (RSTP) uses the term "discarding" for a switch port that is not forwarding frames.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Describe and verify switching concepts

References:

Cisco > Support > LAN Switching > Spanning Tree Protocol > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w) > Document ID: 24062

Question 408

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?

- ☒ no cdp run
- ☐ set cdp disable
- ☐ no cdp enable
- ☐ no cdp advertise-v2

Explanation:

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

 Licensed to Berend Post berend.post@it-university.nl

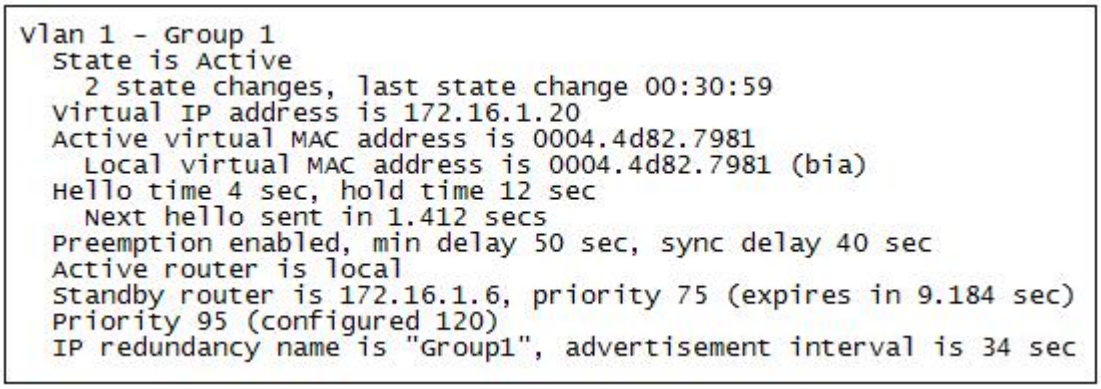
References:

Cisco > Support > Using Cisco Discovery Protocol

Cisco > Support > Technology Support > Network Management > Cisco's Response to the CDP Issue > Document ID: 13621

Question 409

The partial output displayed in the exhibit is a result of what IOS command? (Click on the Exhibit(s) button.)



- ☐ switch# show running-config
- ☐ switch# show standby vlan1 active brief
- ☐ switch# show hsrp 1
- ☒ switch# show standby

Explanation:

Explanation:

The command shows standby produces the output displayed in the exhibit. This command displays information about HSRP on all configured interfaces and for all HSRP groups. Important information in the exhibit includes that this router is the active router, the virtual IP address for the HSRP group is 172.16.1.20, the address of the standby router is 172.16.1.6, and the router is configured to preempt.

The command show running-config will display the complete configuration of the device, including the configuration of HSRP, but will not display the current status of HSRP on the switch.

The command show standby vlan 1 active brief provides a summary display of all HSRP groups on the switch that are in the active state. This output would provide basic information, not nearly the detail indicated in the exhibit. The following is an example of output for show standby vlan 1 active brief:

Interface Grp Prio P State Active addr Standby addr Group addr

 Licensed to Berend Post berend.post@it-university.nl

Vlan1 0 120 Active 172.16.1.5 Unknown 172.16.1.20

The command show hsrp 1 is not valid due to incorrect syntax.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Cisco > Cisco IOS IP Application Services Command Reference > show ip sockets through standby name > show standby

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

Question 410

What is the default administrative distance of a static route?

- ☐ 90
- ☐ 0
- ☒ 1
- ☐ 110

Explanation:

Explanation:

While the administrative distance of a route can be altered, there are default administrative distance values assigned to various methods of learning routes. When a static route is defined, it will have an administrative distance of 1.

An administrative distance value of 90 is the default assigned to EIGRP.

An administrative distance value of 0 is the default assigned to directly connected routes.

An administrative distance value of 110 is the default assigned to OSPF.

Objective:

Licensed to Berend Post berend.post@it-university.nl

Routing Fundamentals

Sub-Objective:

Describe how a routing table is populated by different routing information sources

References:

Support > Technology Support > IP > IP Routing > Troubleshoot and Alerts > Troubleshooting TechNotes > Route Selection in Cisco Routers

Question 411

Which of the following statements are true when discussing link state and distance vector routing protocols? (Choose all that apply.)

- ☐ After convergence, routing advertisements are only triggered by changes in the network with distance vector protocols
- ☒ Packets are routed based upon the shortest path calculated by an algorithm with link state protocols
- ☐ Only one router in an OSPF area can represent the entire topology of the network
- ☒ Distance vector protocols send the entire routing table to a neighbor
- ☐ Distance vector protocols send updates regarding the status of their own links to all routers in the network
- ☒ Link-state protocols place a high demand on router resources running the link-state algorithm
- ☐ Distance vector protocols require a hierarchical IP addressing scheme for optimal functionality
- ☒ Link-state protocols use hello packets and LSAs from other routers to build and maintain the topological database
- ☒ Link-state protocols require a hierarchical IP addressing scheme for optimal functionality.

Explanation:

Explanation:

The following statements are true of link-state and distance vector routing protocols:

Packets are routed based upon the shortest path calculated by an algorithm with link state protocols.

Distance vector protocols send the entire routing table to a neighbor.

Link-state protocols place a high demand on router resources running the link-state algorithm.

Link-state protocols use hello packets and LSAs from other routers to build and maintain the topological database.

Link-state protocols require a hierarchical IP addressing scheme for optimal functionality.

Licensed to Berend Post berend.post@it-university.nl

Link state protocols like OSPF use the Shortest Path First algorithm to calculate the shortest path based on a metric called cost, while distance vector protocols like RIP consider only hop count when determining the best route. Running the algorithm places a high demand on router resources. Distance vector protocols are required to send the entire routing table with each update, while link state protocols only send updates when required by changes in the network. Therefore, less traffic is created with link state protocols.

Sending routing advertisements after convergence only when changes occur in the network is a characteristic of link state protocol's not distance vector protocols. With distance vector protocols, updates occur regularly and include the entire routing table.

All routers in an OSPF area can represent the entire topology of the network, not just one.

Distance vector protocols do not send updates regarding the status of their own links to all routers in the network. Updating link status is a characteristic of link state protocols. Distance vector protocols send the entire routing table.

Distance vector protocols do NOT require a hierarchical IP addressing scheme for optimal functionality. Link-state protocols do require this for optimal functionality, as it supports more efficient route aggregation or summarization. This reduces the number of routes in the table and the number of calculations required by the SPF algorithm, thereby lowering router resource demand.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

Cisco>Internetworking Technology Handbook>Routing Basics>Link-State versus Distance Vector

Licensed to Berend Post berend.post@it-university.nl

Question 412

Examine the output shown below:

```
R1#show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H   Address          Interface Hold Uptime   SRTT   RTO  Q  Seq
                              (sec)         (ms)       Cnt Num
0  Link-local add     Se0/0   13 15:17:58   44     264  0  12
    FE80::2

R2#show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 1
H   Address          Interface  Hold Uptime   SRTT   RTO  Q  Seq
                               (sec)         (ms)       Cnt Num
0   Link-local add    Se0/0    14 16:32:05   30   300  0  12
    FE80::1
```

What is true of this configuration?

- ☐ The link-local address of R1 is FE80::2
- ☒ The link-local address of R1 is FE80::1
- ☐ The area ID is 1
- ☐ No adjacency has formed

Explanation:

Explanation:

The output shows that the link-local address of R1 is FE80::1. R1's link-local address appears in the output of R2 because the show ipv6 eigrp neighbors command displays information about the neighbor, not the local router.

The link-local address of R1 is not FE80::2. That is the link-local address of R2.

Because the area ID is not displayed in the output, we do not know its value. The only 1 in the output is the value representing the process ID of both routers, IPv6-EIGRP neighbors for process 1.

It is not true that no adjacency has formed. There is an adjacency present; if there were not, the two routers would not appear in each other's output of the show ipv6 eigrp neighbors command.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)

Licensed to Berend Post berend.post@it-university.nl

References:

Home > Support > Cisco IOS IPv6 Command Reference > show ipv6 eigrp neighbors

Question 413

Which Cisco IOS command would you use to troubleshoot IP addressing problems?

- ☐ ipconfig /all
- ☐ show config
- ☒ show running-config
- ☐ show config-file

Explanation:

Explanation:

The show running-config command will help troubleshoot IP addressing problems, because it shows the details of the router configuration, including the IP address configured on each interface.

The ipconfig /all command is a Microsoft command used to verify IP address configuration on a workstation running Windows. This is not a valid Cisco command.

The show config command has been replaced by the show startup-config command. Both of these commands are used to display the startup configuration of the router stored in NVRAM.

The show config-file command is not a valid Cisco command.

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

Cisco > Cisco IOS Configuration Fundamentals Command Reference > show gsr through showmon > show running-config

Licensed to Berend Post berend.post@it-university.nl

Question 414

Which WAN switching technology is used with ISDN?

- ☐ packet switching
- ☐ virtual switching
- ☒ circuit switching
- ☐ cell switching

Explanation:

Explanation:

Circuit switching dynamically establishes a connection between a source and a destination. The connection cannot be used by other callers until the circuit is released. Circuit switching is the most common technique used with the public switched telephone network (PSTN) to make phone calls. During a call, a dedicated virtual circuit is temporarily established between the caller and receiver for the duration of the call. Once the caller or receiver hangs up the phone, the circuit is released and is made available for other users.

Packet switching is a technique popularly used for transfer of data that is not delay sensitive and does not require real-time transfer rates from a sender to a receiver. Also unlike circuit switching which makes a fixed amount of bandwidth available for the connection (which may not be fully utilized) packet switching uses bandwidth more efficiently. With packet switching, the data is broken into labeled packets and is transmitted using packet-switching networks.

Cell switching is used by Asynchronous Transfer Mode (ATM). ATM is an International Telecommunication Union-Telecommunications (ITU-T) standard for transmission of data, voice, or video traffic using a fixed size frame of 53 bytes, known as cells. Of these 53 bytes, the initial five bytes are header information and the remaining 48 bytes are the payload. These cells are transmitted over a path that may vary with each cell. It does not maintain a dedicated virtual circuit.

The term "virtual switching" is incorrect because it is not a valid WAN switching technology.

Objective:

WAN Technologies

Sub-Objective:

Describe WAN access connectivity options

References:

Cisco Documentation > Internetworking Technology Handbook > Introduction to WAN Technologies > Circuit Switching

Licensed to Berend Post berend.post@it-university.nl

Question 415

Which command can be issued at the following prompt?

Router(config-router)#

- ☐ show interface
- ☒ network
- ☐ interface
- ☐ ip default-gateway

Explanation:

Explanation:

The network command can be issued at the Router(config-router)# prompt, which also indicates that the router is in router configuration mode. The network command is used to configure the network upon which a routing protocol is functioning.

The router configuration mode is accessed by issuing the router command in the global configuration mode along with a parameter indicating the routing protocol to be configured. For example:

R4(config)#router eigrp 1

changes the prompt to:

R4(config-router)#

which then allows you to specify the network as follows:

R4(config-router)#network 192.18.5.0

All other options are incorrect as these commands can be issued only in the global configuration command mode (which would be indicated by the R4(config)# prompt.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify initial device configuration

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Support > Cisco IOS Software > Using the Command-Line Interface in Cisco IOS Software

Question 416

Which of the following are port roles in the Rapid Spanning Tree Protocol (RSTP)? (Choose three.)

- ☒ Alternate
- ☐ Listening
- ☐ Routing
- ☒ Designated
- ☒ Backup
- ☐ Blocking
- ☐ Discarding

Explanation:

Explanation:

There are five port roles in RSTP:

Root port: the closest port to the root bridge in terms of path cost. There can be only one root port on each switch, and the root switch is the only switch in the network that does not have a root port.

Designated port: a forwarding port to the root bridge. All versions of STP require each network segment to have only one path toward the root bridge, to avoid bridging loops in redundantly connected environments. All bridges connected to a given segment listen to one another's BPDUs and agree that the bridge that is sending the best BPDU is the designated bridge for the segment.

Alternate port: a blocking port that becomes the root port if the active root port fails.

Backup port: a blocking port that becomes the designated port if an existing designated port fails.

Disabled port: a disabled port has no role within the operation of spanning tree.

RSTP was designed to provide rapid convergence of the spanning tree in case of changes to the active topology, such as switch failure.

RSTP has the following similarities to STP:

RSTP elects the root switch using the same parameters as STP.

RSTP elects the root port using the same rules as STP.

Designated ports on each LAN segment are elected in RSTP in the same way as STP.

Listening is a port state, not a port role. Listening is the STP transitional state while a port is preparing to enter a root or designated role.

Blocking is a port state, not a port role. A blocking port is inactive in STP spanning tree, and blocking is not a port state in RSTP. In RSTP that port state is called discarding.

Licensed to Berend Post berend.post@it-university.nl

The routing port does not exist in the RSTP topology.

Discarding is an RSTP port state, not a port role.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Support > Technology Support > LAN Switching > Spanning Tree Protocol > Troubleshoot and Alerts > Troubleshooting TechNotes > Understanding Rapid Spanning Tree Protocol (802.1w)

Question 417

Which two are NOT features of Cisco NAT implementation? (Choose two.)

- ☐ overload
- ☒ override
- ☒ overrule
- ☐ static NAT
- ☐ dynamic NAT

Explanation:

Explanation:

Override and overrule are NOT features of Cisco's Network Address Translation (NAT) implementation. NAT translates internal IP address to external IP address and vice versa. NAT is typically used by firewalls or routers.

The following are some of the characteristics of NAT:

It can act as an address translator between Internet and the local network.

It conserves IP addresses and simplifies the process of IP address allocation.

It allows the local network to connect to Internet using unregistered IP addresses.

It can present only one address for the entire network to the outside world when using dynamic NAT.

It enhances network security, as it does not disclose internal network addresses to the outside world.

All of the other options are incorrect because they are valid NAT features.

 Licensed to Berend Post berend.post@it-university.nl

With static NAT, translation mappings are created statically and are placed in the translation tables whether or not there is traffic flowing. In this case, no registered addresses are saved because a registered address is still required for each mapping.

With dynamic NAT, the translation table is populated as the required traffic flows through NAT-enabled devices. In this case, a single address or multiple public addresses can be used multiple times to represent multiple private addresses.

The overload keyword allows the ip nat inside command to translate multiple devices in the internal network to the single address in the IP address pool. This process is also called overloading in that the same public IP address is mapped to all private addresses from inside the network. Since the router performing the NAT overload function will use the unique TCP source port from each host for identification, while mapping all of them to the same public IP address, it is sometimes referred to as Port Address Translation or PAT.

For example:

ip nat pool test 172.28.15.1 172.28.15.1 prefix 24

In this example, the NAT pool named "test" only has a range of one address.

Another variant of this command is given below, which configures NAT to overload on the address assigned to the serial 0 interface:

ip nat inside source list 3 interface serial 0 overload

When this variation is used, the command uses a list named 3 to determine the addresses in the pool.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot inside source NAT

References:

Licensed to Berend Post berend.post@it-university.nl

Cisco > Technology Support > IP > IP Routing > Design Technotes > Configuring Network Address Translation: Getting Started > Document ID: 13772 > Quick Start Steps for Configuring and Deploying NAT

Question 418

Which of the following technologies allows a switch port to immediately transition to a forwarding state?

- ☐ Rapid STP
- ☒ PortFast
- ☐ VTP
- ☐ CDP

Explanation:

Explanation:

PortFast is a technology that allows a switch port connected to an end node such as a workstation, server, or printer to bypass the normal Spanning Tree Protocol (STP) convergence process. When a new device is powered up on a switch port, it will immediately transition to a forwarding state.

NOTE: PortFast should only be used on access ports. It should not be used on trunk ports or on ports that connect to hubs, routers and other switches.

Rapid STP (RSTP) is a new STP standard that provides faster convergence than the original 802.1d STP. RSTP supports PortFast, but it must be configured explicitly.

The VLAN Trunking Protocol (VTP) does not allow for immediate transition to a forwarding state. VTP is used to synchronize VLAN databases between switches, and has no effect on STP.

The Cisco Discovery Protocol (CDP) does not allow for immediate transition to a forwarding state. CDP is used to verify connectivity and document directly connected Cisco devices. CDP is not related to STP.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP-related optional features

References:

 Licensed to Berend Post berend.post@it-university.nl

Cisco > Support > Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, and LoopGuard > Understanding How PortFast Works

Question 419

Which media access control method is used by Ethernet technology to minimize collisions in the network?

- ☒ CSMA/CD
- ☐ token passing
- ☐ back-on algorithm
- ☐ full-duplex

Explanation:

Explanation:

Carrier Sense Multiple Access - Collision Detection (CSMA/CD) is used by Ethernet technology to minimize collisions in the network. The CSMA/CD method uses a back-off algorithm to calculate random time for retransmission after a collision. When two stations start transmitting at the same time, their signals will collide. The CSMA/CD method detects the collision, and both stations hold the retransmission for a certain amount of time that is determined by the back-off algorithm. This is an effort to help ensure that the retransmitted frames do not collide.

Token passing is used by the token-ring network topology to control communication on the network.

Full-duplex is the Ethernet communication mode that allows workstation to send and receive simultaneously. With the use of full-duplex, the bandwidth of the station can effectively be doubled. Hubs are not capable of handling full-duplex communication. You need dedicated switch ports to allow full-duplex communication.

The back-on algorithm is an invalid option. There is no such contention method.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Cisco Documentation > Internetworking Technology Handbook > Ethernet Technologies

 Licensed to Berend Post berend.post@it-university.nl

Question 420

What is the purpose of using the show arp command?

- ☐ To view the ARP statistics only for a particular interface
- ☐ To view details regarding neighboring devices discovered by ARP
- ☐ To view global ARP information such as timer and hold time
- ☒ To view the Address Resolution Protocol (ARP) cache

Explanation:

Explanation:

The show arp command is used to view the Address Resolution Protocol (ARP) cache. ARP is used by the Internet Protocol (IP) to find the Media Access Control (MAC) address or the hardware address of a host. The main function of ARP is to translate IP addresses to MAC addresses. The process of obtaining the address of a computer in the network is known as address resolution. This process is accomplished by sending an ARP packet from a source to a destination host. The destination host responds to the ARP packet by replying back to the source and including its own MAC address. Once the source host receives the reply, it will update its ARP cache with the new MAC address.

The complete syntax of the show arp command is:

show arp [ip-address [locationnode-id] | hardware-address [locationnode-id] | traffic [locationnode-id | interface-instance] | trace [error [locationnode-id] | dev [locationnode-id] | events [locationnode-id] table [locationnode-id] packets [locationnode-id] | [locationnode-id]] | type instance| [locationnode-id]

The following is a brief description of the parameters used with this command:

ip-address: An optional parameter that displays specific ARP entries.

locationnode-id: An optional parameter that displays the ARP entry for a specific location. The method for entering the node-id argument is rack/slot/module notation.

hardware-address: An optional parameter that displays ARP entries that match the 48-bit MAC address.

traffic: An optional parameter that displays ARP traffic statistics.

interface instance: Either a physical interface instance or a virtual interface instance:

Physical interface instance: the naming notation is rack/slot/module/port and a slash mark between values is required as part of the notation where:

rack refers to the chassis number of the rack.

slot refers to the physical slot number of the line card.

module refers to the module number. A physical layer interface module (PLIM) is always 0.

 Licensed to Berend Post berend.post@it-university.nl

port refers to the physical port number of the interface.

Virtual interface instance: the number range is variable depending on the type of interface.

trace: An optional parameter that displays the ARP entries in the buffer.

error: An optional parameter that displays the ARP error logs.

dev: An optional parameter that displays the ARP internal logs.

events: An optional parameter that displays the ARP events logs.

table: An optional parameter that displays the ARP cache logs.

packets: An optional parameter that displays the ARP packet receive and reply logs.

type instance: An optional parameter that specifies the interface for which you want to view the ARP cache.

An example of the output of the show arp command is shown below along with a diagram of the network in which the router resides.

R1#show arp

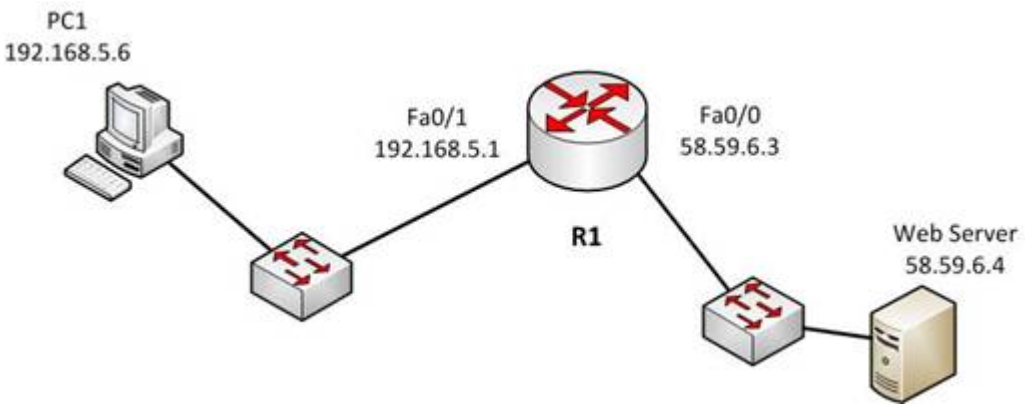
Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.0.5.1 120 0000.a710.4baf ARPA FastEthernet 0/1

Internet 192.0.5.6 105 0000.a710.859b ARPA FastEthernet 0/1

Internet 58.59.6.3 42 0000.a710.68cd ARPA FastEthernet 0/0

Internet 58.59.6.4 59 0000.0c01.7bbd ARPA FastEthernet 0/0



Licensed to Berend Post berend.post@it-university.nl

From the information above, we can make the following conclusions about the actions R1 will take when it receives data from PC1 destined for the Web server:

The data frames will be forwarded out the Fa0/0 interface of R1

R1 will place the MAC address of the Web Server (0000.0c01.7bbd) in the destination MAC address of the frames

R1 will put the MAC address if the forwarding Fa0/0 interface (0000.a710.68cd) in the place of the source MAC address

The option stating that the show arp command is used to view the ARP statistics only for a particular interface is incorrect because this command is used to view the ARP cache. You can also view the information for a particular interface with the help of the interface instance parameter.

The options stating that the show arp command is used to view the details of neighboring devices discovered by the ARP or to view global ARP information, such as hold time and timer, are both incorrect because these are both Cisco Discovery protocol (CDP) functions, not ARP functions. The show cdp neighbors detail command is used to display details regarding the neighboring devices that are discovered by CDP, and the show cdp command displays global CDP information, such as timer and hold-time.

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv4 addressing and subnetting

References:

Question 421

At which of the following layers of the Cisco three-tier architecture should port security be implemented?

- ☒ Access layer
- ☐ Distribution layer
- ☐ Core layer
- ☐ Edge layer

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Port security is one of the functions that should be performed at the Access layer. Among other functions that are done at this layer are:

PoE

Link aggregation

QoS

Port security should not be performed at the Distribution layer. Among the functions that should be done at this layer are:

Routing updates

Route summaries

VLAN traffic

Address aggregation

Port security should not be performed at the Core layer. Among the functions that should be done at this layer are:

Access-list checking

Data encryption

Address translation

Edge is not one of the three layers in the Cisco three-tier model.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast collapsed core and three-tier architectures

References:

Cisco Press > Articles > Cisco Network Technology > General Networking > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network DesignStudy CCNA > Cisco three-layer hierarchical model

Licensed to Berend Post berend.post@it-university.nl

Question 422

You have two routers in your OSPF area 0. Router 1 is connected to Router 2 via its Serial 1 interface, and to your ISP via the Serial 0 interface. Router 1 is an ASBR.

After your assistant configures a default route on Router 1, you discover that whenever either router receives packets destined for networks that are not in the routing tables, it causes traffic loops between the two routers.

To troubleshoot, you execute the show run command on Router 1. Part of the output is shown below:

<output omitted>
IP route 0.0.0.0 0.0.0.0 serial 1
Router ospf 1
Network 192.168.5.0 0.0.0.255 area 0
Default-information originate

Which command or set of commands should you execute on Router 1 to stop the looping traffic while maintaining Router 2's ability to send traffic to the Internet?

- ☐ Execute the no default-information originate command.
- ☒ Execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command and then execute the ip route 0.0.0.0 0.0.0.0 serial 0 command.
- ☐ Execute the default-information originate always command.
- ☐ Execute the no network 192.168.5.0 area 0 command and then execute the network 192.168.5.0 255.255.255.0 area 0 command.

Explanation:

Explanation:

You should execute the no ip route 0.0.0.0 0.0.0.0 serial 1 command followed by the ip route 0.0.0.0 0.0.0.0 serial 0 command. The original configuration command was executed on the wrong interface on Router 1 by your assistant. It should be executed on Serial 0, which is the connection to the ISP. The show run command indicates that with the current configuration, if Router 2 receives a packet not in its table, it sends it to Router 1, and then Router 1 sends it back out on Serial 1. This redirects the packet back to Router 2, and the loop begins. By changing the configuration to Serial 0, Router 1 will start forwarding all traffic not in the routing table to the ISP.

You should not execute the no default-information originate command. This command instructs Router 1 to NOT inject the default route into area 0, which is the desired behavior. Running this command would stop the loop, but would leave Router2 with no default route to send packets to the Internet.

You should not execute the default-information originate always command. It will not change the existing looping behavior. The addition of the always parameter instructs Router 1 to inject a default route into area 0, even if one does not exist on Router 1. This is unnecessary, since Router 1 does

 Licensed to Berend Post berend.post@it-university.nl

have a default route configured, and will not change the existing looping behavior. To advertise a default route to other OSPF routers, you should run this command:

Router1(config-router)#default information originate

You should not execute the no network 192.168.5.0 area 0 command followed by the network 192.168.5.0 255.255.255.0 area 0 command. There is nothing wrong with the original network command. Also, the network 192.168.5.0 255.255.255.0 area 0 command uses an incorrect mask type. The mask must be in the wildcard format. Moreover, since it is incorrect, this will have the effect of disabling OSPF on the network connecting the two routers.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Cisco > Home > Support > Technology Support > IP > IP Routing > Configure > Configurations Examples and Technotes > How OSPF Injects a Default Route into a Normal Area

Question 423

Which of the following accurately describes the purpose of a trunk?

- ☐ A trunk is used to carry traffic for a single VLAN and is typically used between switches.
- ☐ A trunk is used to carry traffic for a single VLAN and is typically used between a switch and an end-user device.
- ☒ A trunk is used to carry multiple VLANs and is typically used between switches.
- ☐ A trunk is used to carry multiple VLANs and is typically used between a switch and a server.

Explanation:

Explanation:

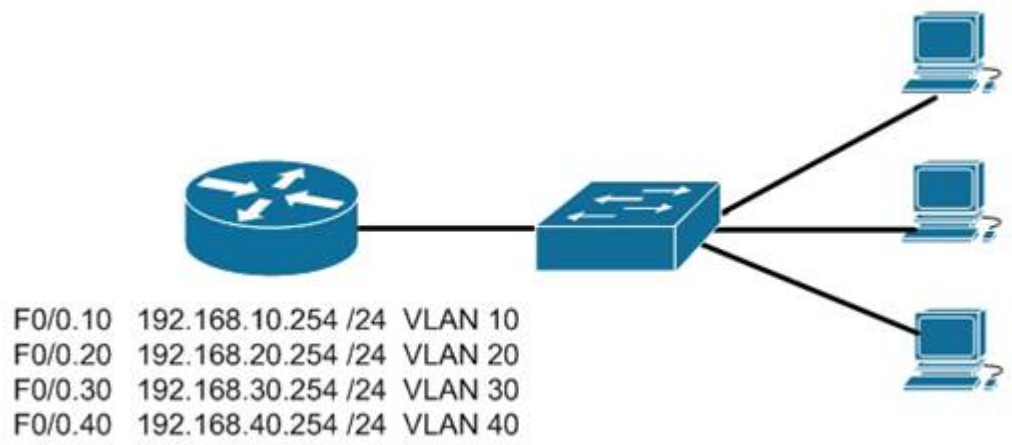
Trunk links are used between switches to allow communications between hosts that are in the same VLAN, but connected to different switches. Trunk links do not allow hosts in different VLANs to communicate, unless there is an additional trunk link connecting to a Layer 3 device, such as a router or a 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

 Licensed to Berend Post berend.post@it-university.nl

in VLAN 20 on SwitchB. A trunk link supports all VLANs by default, and frames that are not traveling on the native VLAN are "tagged" with the VLAN ID of the originating port before being sent over the trunk. The receiving switch reads the VLAN ID and forwards the frame to the appropriate host in the same VLAN.

The other options are incorrect because trunk links do not carry data for a single VLAN, nor are trunks used between switches and hosts (such as workstations and servers).

When a trunk link is extended to a router for the purpose of enabling routing between VLANs, the physical connection that the link connects to is usually subdivided logically into subinterfaces. Then each subinterface is given an IP address from the same subnet as the computers that reside on that VLAN. Finally, each computer in the VLAN will use the corresponding IP address on the matching subinterface of the router as its default gateway. In the example below, the switch has five VLANs created and some hosts connected to it. If hosts from different VLANs need to communicate, the link between the router and the switch must be a trunk link.



Furthermore, the physical link on the router must be subdivided into subinterfaces and addressed according to the legend shown for each subinterface in the diagram. For example, the configuration for VLAN 10 shown in the diagram would be as follows:

Router(config)# interface f0/0.10

Router(config-if)#encapsulation dot1q 10

Router(config-if)#ip address 192.168.10.254 255.255.255.0

Finally, each computer in VLAN 10 should have its default gateway set to 192.168.10.254.

Licensed to Berend Post berend.post@it-university.nl

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Question 424

When a router has been configured with a loopback address, which of the following determines the OSPF router ID?

- ☐ The highest MAC address assigned to a physical interface on the router
- ☐ The lowest priority of a physical interface on the router
- ☐ The lowest IP address assigned to a physical interface on the router
- ☒ The highest IP address assigned to a loopback interface on the router

Explanation:

Explanation:

Routers configured with OSPF must be assigned a router ID (RID), which is an IP address unique across the entire OSPF autonomous system. The RID can be assigned manually with the router-id command, or it will be determined automatically by OSPF. If the RID has not been manually assigned, then OSPF will use the highest numerical IP address of a loopback interface on the local router. If there are no configured loopback interfaces, then the RID will be determined by the highest numerical IP address on an active physical interface. The sequence for determining the RID is as follows:

Any address manually configured with the router-id command

The highest IP address on a loopback interface

The highest IP address on an active physical interface

Either of the first two options would be a recommended best practice, since they each offer fault tolerance to the RID. If the RID is determined by a physical interface IP address, then the entire OSPF routing process is bound to an interface that could become unplugged or go down due to network reasons.

Loopback interfaces remain operational unless they are manually shut down. Loopback interfaces are configured as follows:

Router(config)# interface loopback0

Licensed to Berend Post berend.post@it-university.nl

Router(config-if)# ip address 192.168.1.254 255.255.255.255

The highest media access control (MAC) address assigned to a physical interface on the router is not used. IP addresses are used for the determination of the router ID.

Priorities are not used to determine the OSPF router ID. Priorities are used by OSPF to influence the election of the designated router (DR) and backup designated router (BDR) on a multi-access segment.

Router IDs are determined by the highest IP address on a loopback or physical interface, not the lowest.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Question 425

Which Cisco Internetwork Operating System (IOS) command is used to assign a router a name for identification?

- ☐ description
- ☐ banner motd
- ☒ hostname
- ☐ banner exec

Explanation:

Explanation:

The hostname command is used to assign the router a name for identification. This command is a global configuration mode command. The syntax of the command is as follows:

Router(config)# hostname [name]

The name parameter of the command specifies the new host name for the router.

 Licensed to Berend Post berend.post@it-university.nl

The description command is incorrect because this command is used to set a description for an interface. The description command is an interface configuration mode command.

The banner motd command is used to specify a message of the day (MOTD) banner to users logging into the router. This is a global configuration mode command, but it does not assign a name to the router for identification.

The banner exec command enables a banner message to be displayed when an EXEC process is created; for example, if a line is activated or an incoming connection is made to a telnet line.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify initial device configuration

References:

Cisco > Cisco IOS Configuration Fundamentals Command Reference > F through K > hostname

Question 426

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)?

- ☒ router# copy running-config startup-config
- ☐ router(config)# copy running-config startup-config
- ☐ router# copy startup-config running-config
- ☐ router(config)# copy startup-config running-config

Explanation:

Explanation:

The router# copy running-config startup-config command is used to copy the configuration stored in Random Access Memory (RAM) to Non-Volatile Random Access Memory (NVRAM). This command is issued in privileged EXEC mode. The syntax of the command is as follows:

router# copy running-config startup-config

The parts of the command are as follows:

running-config is the running configuration stored in RAM.

 Licensed to Berend Post berend.post@it-university.nl

startup-config is the startup configuration stored in Non-Volatile Random Access Memory (NVRAM).

The router(config)# copy running-config startup-config command is incorrect because the copy run start command (abbreviated) is not issued in global configuration mode. It is executed in privileged EXEC mode.

The router# copy startup-config running-config command is incorrect because this command is used to copy the configuration stored in NVRAM to RAM.

The router(config)# copy startup-config running-config command is incorrect because neither the copy run start nor the copy start run commands are executed in global configuration mode. Moreover, the copy startup-config running-config command is used to copy the configuration stored in NVRAM to RAM.

Objective:

Infrastructure Management

Sub-Objective:

Perform device maintenance

References:

Cisco > Support > IOS and Configuration Basics > Saving Configuration Changes

Question 427

What are the three types of Internet Protocol version 6 (IPv6) addresses? (Choose three.)

- ☒ Unicast
- ☐ Broadcast
- ☐ Dual-cast
- ☒ Anycast
- ☒ Multicast

Explanation:

Explanation:

Unicast, multicast, and anycast are types of IPv6 addresses.

The following are the IPv6 address types:

Licensed to Berend Post berend.post@it-university.nl

Unicast address: These types of addresses are used to define a single destination interface. A packet sent to a unicast address is delivered to the specific interface.

Multicast address: These types of addresses are used to define a group of hosts. When a packet is sent to a multicast address, it is delivered to all the hosts identified by that address. Multicast addresses begin with the prefix FF00::/8 and the second octet identifies the range over which the multicast address is propagated. Some special case IPv6 multicast addresses:

- FF01:0:0:0:0:0:0:1: Indicates all-nodes address for interface-local scope.

- FF02:0:0:0:0:0:0:2: Indicates all-routers address for link-local.

Anycast address: These types of addresses are used to identify a set of devices. These addresses are also assigned to more than one interface belonging to different nodes. A packet sent to an anycast address is delivered to just one of the interfaces, based on which one is closest. For example, if an anycast address is assigned to a set of routers, one in India and another in the U.S., the users in the U.S. will be routed to U.S. routers and the users in India will be routed to a server located in India.

The broadcast option is incorrect because these types of addresses are not supported by IPv6. Broadcast functionality is provided by multicast addressing.

The dual-cast option is incorrect because this is not a valid Cisco address type.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast IPv6 address types

References:

Licensed to Berend Post berend.post@it-university.nl

Question 428

You are configuring an authenticated connection between two routers named Tacoma and Lansing. The connection on the Lansing end is correctly set up with a password of keypass. You are directing an assistant to configure the name and password on Tacoma.

Which of the following commands would be correct to complete this authenticated connection?

- ☐ username Tacoma password keypass
- ☐ username Lansing keypass password
- ☐ username Tacoma keypass password
- ☒ username Lansing password keypass

Explanation:

Explanation:

To complete the configuration, you should run the command username Lansing password keypass. This command creates a user account for the Lansing router with a password of keypass.

When creating an authenticated connection between the routers, a user account must be created for the other router. The password configured must match on both ends.

When examining the output produced by the show running-configuration command for two routers, the output should read as below:

```
Tacoma# show running-config
<some output text omitted>

enable password cisco
!
hostname Tacoma
username Lansing password keypass
!
```

```
Lansing# show running-config
<some output text omitted>

enable password cisco1
!
hostname Lansing
username Tacoma password keypass
!
```

The lines that display enable password cisco and enable password cisco1 represent local passwords to enable privileged mode on the local router. These passwords do not have to match. The lines of output that must display matching passwords are username Lansing password keypass and username Tacoma password keypass.

You should not run the command username Tacoma password keypass. The username Tacoma portion of the command will create an account named Tacoma. You need an account for the other router, Lansing.

Licensed to Berend Post berend.post@it-university.nl

You should not run the command username Lansing keypass password. The password portion of the command must follow the syntax password [correct_password].

You should not run the command username Tacoma keypass password. The username Tacoma portion of the command will create an account for the wrong router, and the password portion of the command must follow the syntax password [correct_password].

Objective:

WAN Technologies

Sub-Objective:

Configure and verify PPP and MLPPP on WAN interfaces using local authentication

References:

Cisco > Support > WAN > Point-to-Point Protocol (PPP) > Design Technotes > Understanding and Configuring PPP CHAP Authentication > Document ID: 25647

Question 429

You need to configure Network Address Translation (NAT) to allow users access to the Internet. There are 62 private hosts that need Internet access using the private network 10.4.3.64 /26, and all of them will be translated into the public IP address of the serial interface.

Which of the following NAT configurations will allow all 62 hosts to have simultaneous Internet access?

- ☐ Router(config)# ip nat pool POOLNAME 10.4.3.64 /26
- ☐ Router(config)# interface s0
- ☐ Router(config-if)# ip nat inside source 1 pool POOLNAME overload
- ☐ Router(config)# access-list 1 permit 10.4.3.64 0.0.0.127
- ☐ Router(config)# interface s0/0
- ☐ Router(config-if)# ip nat source list 1 pool POOLNAME overload
- ☐ Router(config)# access-list 1 permit 10.4.3.64 /26
- ☐ Router(config)# ip nat inside source list 1 interface serial 0
- ☒ Router(config)# access-list 1 permit 10.4.3.64 0.0.0.63
- ☒ Router(config)# ip nat inside source list 1 interface serial 0 overload

Explanation:

Explanation:

You should execute the following commands:

Licensed to Berend Post berend.post@it-university.nl

Router(config)# access-list 1 permit 10.4.3.64 0.0.0.63

Router(config)# ip nat inside source list 1 interface serial 0 overload

A successful NAT configuration requires the creation of an access control list (ACL) to identify the private IP addresses that will be translated, as well as an ip nat inside source command to dictate what public IP addresses will be used for translation. Cisco uses the term "inside local" for IP addresses prior to translation, and "inside global" for public IP addresses after translation.

The access-list 1 permit 10.4.3.64 0.0.0.63 command correctly identifies the private host network of 10.4.3.64 /26, consisting of 62 hosts.

The ip nat command is broken down as follows:

inside: indicates that packets received on the inside (private) interface will be translated

list 1: specifies that access list 1 will be used to determine which private IP addresses will be translated

interface serial 0: specifies that NAT will translate private IP addresses into the IP address of the serial 0 interface

overload: allows NAT to reuse the IP address of the serial interface for all private IP addresses, providing them simultaneous access to the Internet

The correct wildcard mask is critical to ensuring that the access list allows translation of all LAN devices. For example, if the private LAN used the 192.168.9.0/24 network and 167 devices were present in the network, the correct wildcard mask would be 0.0.0.255. If you used an incorrect wildcard mask, such as 0.0.0.3, only the 192.168.9.0/30 network would be allowed translation (only the IP addresses 192.18.9.1 and 192.168.19.2.) Of the 167 devices, 165 would not receive translation.

The overload keyword is required in this configuration, since there are more private IP addresses (62) than there are public IP addresses (one). Overload activates NAT overloading, often called Port Address Translation (PAT), and assigns each private IP address a unique, dynamic source port in router memory to track connections. If the overload keyword were not included in the NAT configuration, only one private host could access the Internet at a time.

An alternate solution would involve the creation of a pool of public IP addresses on the NAT router, and applying the access control list to the NAT pool:

Router(config)# ip nat pool NATPOOL 201.52.4.17 201.52.4.22 netmask 255.255.255.248

Router(config)# ip nat inside source list 1 pool NATPOOL overload

 Licensed to Berend Post berend.post@it-university.nl

The first command creates a NAT pool with six public IP addresses on subnet 201.52.4.16/29, which will be used for translation. The second command then ties access list 1 to the NAT pool, and specifies overload so that the six public addresses can be reused as often as necessary, allowing all of the private IP addresses simultaneous Internet access.

In both of these examples, dynamic mapping is used. Without dynamic mapping, it is not possible for computers from outside the network to establish a connection with computers inside the network unless a static mapping between the private IP address and the public IP address is established on the NAT device.

A common alternative approach is to use public IP addresses in the DMZ rather than private IP addresses, and to place any computers than must be accessed from outside the network in the DMZ. In this case, NAT is not required between the DMZ devices and the Internet. Even if public IP addresses are used in the DMZ, if the addresses undergo NAT translation, connections from outside the network will not be possible.

When NAT is used to translate a public IP address (or addresses) to private IP addresses, the NAT process is ONLY implemented on the router that connects the network to the Internet. This is because private IP addresses are not routable to the Internet, and translation must occur where the network connects to the Internet.

The following command sets are incorrect because they both involve the creation of a NAT pool:

Router(config)# ip nat pool POOLNAME 10.4.3.64 /26

Router(config)# interface s0

Router(config-if)# ip nat inside source 1 pool POOLNAME overload

and

Router(config)# access-list 1 permit 10.4.3.64 0.0.0.127

Router(config)# interface s0/0

Router(config-if)# ip nat source list 1 pool POOLNAME overload

The scenario states you must use the IP address of the serial interface as the public address. Also, the ip nat inside source command is configured in global configuration mode, not interface configuration mode. Finally, access control lists require inverse masks (such as 0.0.0.63). CIDR notation (as in POOLNAME 10.4.3.64 /26) is not allowed.

 Licensed to Berend Post berend.post@it-university.nl

The following command set is incorrect because access control lists require inverse masks (such as 0.0.0.63) and CIDR notation (/26) is not allowed:

Router(config)# access-list 1 permit 10.4.3.64 /26

Router(config)# ip nat inside source list 1 interface serial 0

Also, the ip nat inside source command is configured in global configuration mode, not interface configuration mode.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot inside source NAT

References:

Question 430

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.)

- ☐ The prompt is incorrect on line 1
- ☒ The IP address is missing a subnet mask
- ☐ The prompt is incorrect on line 5
- ☒ The prompt is incorrect on line 3
- ☒ The command on line 4 is incorrect
- ☐ The prompt is incorrect on line 4
- ☐ The description command must be executed before the interface is enabled

Explanation:

Explanation:

 Licensed to Berend Post berend.post@it-university.nl

The IP address is missing a subnet mask, the prompt is incorrect on line 3, and the command enabling the interface (line 4) is incorrect.

The correct prompts and commands are as follows:

Router# configure terminal

Router(config)# interface S0

Router(config-if)# ip address 192.168.5.5 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# description T1 to Raleigh

The prompt for line 3 would be Router(config-if)# because the interface S0 command was issued immediately prior to the ip address 192.168.5.5 command. The prompt will remain Router(config-if)# for lines 3, 4, and 5 as each command that applies to the S0 interface is executed, including the description command.

The command to enable the interface is no shutdown, not enable interface. Therefore, the command executed on line 4 was incorrect.

Objective:

Network Fundamentals

Sub-Objective:

Apply troubleshooting methodologies to resolve problems

References:

Home > Support > Using the Command-Line Interface in Cisco IOS Software

Licensed to Berend Post berend.post@it-university.nl

Question 431

Consider the following output of the show ip interface brief command:

```
R1# show ip interface brief

Interface    IP-Address      OK?   Method   Status    Protocol
Ethernet0    192.168.12.65   YES   manual    up         up
Ethernet1    192.168.12.129  YES   manual    up         up
Serial0      192.168.12.187  YES   manual    up         up
Serial1      192.168.12.125  YES   manual    up         up
Serial2      192.168.12.121  YES   manual    up         up
Serial3      unassigned      YES   unset     up         up
```

You have a single area OSPF network. What command should you execute on R1 so that OSPF is operational on the E0, S1, and S2 interfaces ONLY?

- ☐ R1(config-router)#network 192.168.12.64 0.0.0.127 area 0
- ☒ R1(config-router)#network 192.168.12.64 0.0.0.63 area 0
- ☐ R1(config-router)#network 192.168.12.64 0.0.0.66 area 0
- ☐ R1(config-router)#network 192.168.12.64 255.255.255.192 area 0
- ☐ R1(config-router)#network 192.168.12.64 0.0.0.63 area1

Explanation:

Explanation:

The command R1(config-router)#network 192.168.12.64 0.0.0.63 area 0 would ensure that OSPF is operational on the E0, S1, and S2 interfaces only. When executing the network command in OSPF, a wildcard mask in combination with the network ID used in the command determines which interfaces will participate in OSPF. Any interfaces that are included in the network created by the network ID and the mask will participate in OSPF.

Wildcard masks in OSPF network statements are expressed inversely, and not as a regular subnet masks. For example, if the network you are configuring for OSPF operation is 192.168.10.0/24, then the inverse version of a /24 mask (or 255.255.255.0) would be 0.0.0.255.

The network ID is the starting point and the wildcard mask specifies where the network will end or the range of the network. In this case, the network begins at 192.168.12.64. The value in the last octet of the mask indicates the number of values (including 64) that will be included in the network, which means that it will range from 192.168.12.64 - 192.168.12.127. 64 to 127 equals 64 values if you include the endpoints 64 and 127.

The network, and therefore the operation of OSPF, includes the interfaces E0 (192.168.12.65), S1 (192.168.12.125), and S2 (192.168.12.121) because these three IP addresses lie within the range 192.1268.12.64 - 192.168.12.127.

Licensed to Berend Post berend.post@it-university.nl

The command R1(config-router)#network 192.168.12.64 0.0.0.127 area 0 is incorrect because the resulting network would range from 192.168.12.64 - 192.168.12.191. This would include all of the required interfaces, but would also include E1 (192.168.12.129) and S0 (192.18.12.187), which is not desired.

The command R1(config-router)#network 192.168.12.64 0.0.0.66 area 0 is incorrect because the resulting network would range from 192.168.12.64 - 192.168.12.129. This would include all of the required interfaces, but would also include E1 (192.168.12.129).

The command R1(config-router)#network 192.168.12.64 255.255.255.192 area 0 is incorrect because the mask, while correct in its breadth and the exact inverse of the wild card mask 0.0.0.63, is not stated in wildcard mask format.

The command R1(config-router)#network 192.168.12.64 0.0.0.63 area 1 is incorrect because it specifies area 1. At least one area of an OSPF network must be area 0 and since this is a single area OSPF network, the command must specify area 0.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Cisco > Home > Support > Technology Support > IP > IP Routing > Technology Information > Technology White paper > OSPF Design Guide > Enabling OSPF on the Router

Licensed to Berend Post berend.post@it-university.nl

Question 432

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.)

- ☒ interface vlan 1
- ☒ ip address 192.168.20.244 255.255.255.240
- ☒ no shutdown
- ☒ exit
- ☒ ip default-gateway 192.168.20.241
- ☒ line vty 0 15
- ☒ password cisco
- ☒ login
- ☒ exit
- ☐ interface fastethernet 0/1
- ☐ ip address 192.168.20.244 255.255.255.240
- ☐ no shutdown
- ☐ exit
- ☐ ip default-gateway 192.168.20.241
- ☐ line vty 0 15
- ☐ password cisco
- ☐ login
- ☐ exit
- ☐ interface vlan 1
- ☐ ip address 192.168.20.244 255.255.255.240
- ☐ no shutdown
- ☐ exit
- ☐ ip route 192.168.20.241
- ☐ line vty 0 15
- ☐ login
- ☐ exit
- ☐ 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
- ☐ interface vlan 1
- ☐ ip address 192.168.20.244 255.255.255.240
- ☐ no shutdown
- ☐ exit
- ☐ ip default-gateway 192.168.20.27

Licensed to Berend Post berend.post@it-university.nl

- ☐ line vty 0 15
- ☐ password cisco
- ☐ login
- ☐ exit
- ☐ 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

Explanation:

Explanation:

The following command set is correct:

interface vlan 1

ip address 192.168.20.244 255.255.255.240

no shutdown

exit

ip default-gateway 192.168.20.241

line vty 0 15

password cisco

login

exit

It sets an IP address for VLAN 1, which is the management VLAN. Next, it sets a default gateway that is in the same network with the IP address. It correctly enables the interface, sets a required password on the VTY lines, and sets the switch to prompt for the password.

Switches do not need IP addresses unless you want to remotely manage the devices. When an IP address is assigned to a switch for this purpose, it is not applied to a physical interface. It is applied to the VLAN 1 interface, which is the management VLAN by default.

The following command set is incorrect because it applies the IP address to the fastethernet 0/1 interface, rather than the management VLAN. When you set an IP address for the switch, you do so on the management VLAN, not one of the physical interfaces.

 Licensed to Berend Post berend.post@it-university.nl

interface fastethernet 0/1

ip address 192.168.20.244 255.255.255.240

no shutdown

exit

ip default-gateway 192.168.20.241

line vty 0 15

password cisco

login

exit

The following command set is incorrect because it does not set a password on the VTY lines, which is required to connect with Telnet unless you include the no login command.

interface vlan 1

ip address 192.168.20.244 255.255.255.240

no shutdown

exit

ip default-gateway 192.168.20.241

line con 0 15

login

exit

The following command set is incorrect because it sets the password in the console line rather than the VTY lines.

interface vlan 1

ip address 192.168.20.244 255.255.255.240

no shutdown

exit

ip default-gateway 192.168.20.241

line con 0 15

password cisco

Licensed to Berend Post berend.post@it-university.nl

login

exit

The following command set is incorrect because the address for VLAN1 and the gateway are not in the same subnet. With a 28-bit mask the interval is 16, which means the network that the gateway is in is the 192.168.20.16/28 network and VLAN 1 is in the 192.1683.20.240/28 network.

interface vlan 1

ip address 192.168.20.244 255.255.255.240

no shutdown

exit

ip default-gateway 192.168.20.27

line vty 0 15

password cisco

login

exit

The following command set is incorrect because the VLAN 1 interface has been disabled with the shutdown command.

interface vlan 1

ip address 192.168.20.244 255.255.255.240

shutdown

exit

ip default-gateway 192.168.20.241

line vty 0 15

password cisco

login

exit

Objective:

Infrastructure Management

Licensed to Berend Post berend.post@it-university.nl

Sub-Objective:

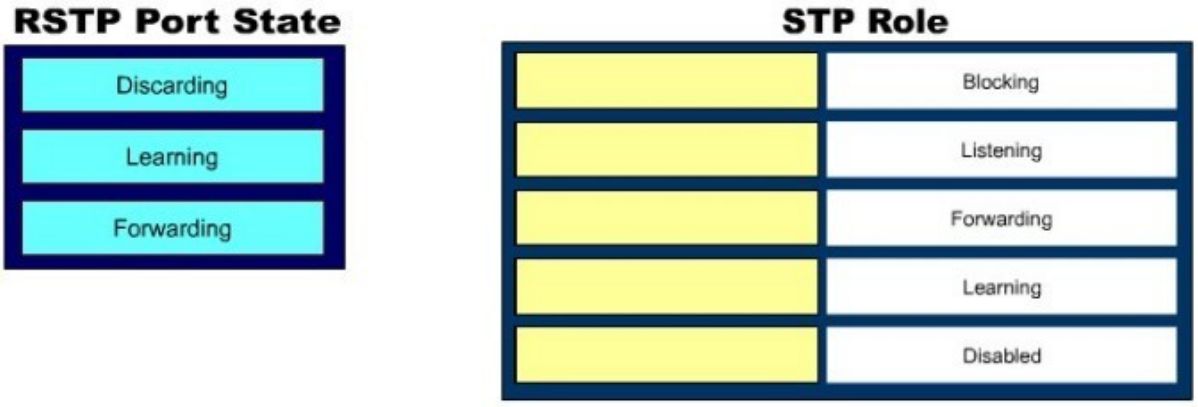
Configure and verify device management

References:

Home>Support>Product Support>End-of-Sale and End-of-life Products>Cisco Catalyst 6000 Series Switches>Troubleshoot and Alerts> Troubleshooting TechNotes>Configuring a Management IP Address on Catalyst 4500/4000, 5500/5000, 6500/6000, and Catalyst Fixed Configuration Switches

Question 433

DRAG DROP
Click and drag the RSTP port state on the left to its matching equivalent STP role, on the right. RSTP port states may be used more than once, and it may not be necessary to use all RSTP port states.



Solution:



Explanation:

Explanation:

Rapid Spanning Tree Protocol (RSTP) was developed to reduce the high convergence times required in Spanning Tree Protocol (STP), and introduces the alternate port and backup port. RSTP is an Institute of Electrical and Electronics Engineers (IEEE) standard, 802.1w, and is interoperable with

Licensed to Berend Post berend.post@it-university.nl

802.1d (STP). There are fewer transitional states used in RSTP than STP. In RSTP, there are only Forwarding, Learning, and Discarding. The three states are defined as follows:

Forwarding - the state of all root ports and designated ports. The port is passing traffic.

Learning - the state of a port that was formerly discarding but due to a change in the topology (link down) it has transitioned to learn its new state. The port could return to discarding or move to forwarding depending on the new topology needs

Discarding - the state of all non-root and non- designated ports. The port is not passing traffic to prevent potential switching loops.

RSTP can reconfigure the spanning tree in less than a second, compared to the 50 seconds that STP may take. This is achieved through having fewer transition states, the use of alternate and backup ports, and faster transitions.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot STP protocols

References:

Cisco > Technology Support > LAN Switching > Spanning Tree Protocol > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w)

Cisco Support > Technology Support > LAN Switching > Spanning Tree Protocol > Troubleshoot and Alerts > Troubleshooting TechNotes > Understanding Rapid Spanning Tree Protocol (802.1w)

CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125, 2nd Edition, Chapter 2: LAN Switching Technologies - Configure, verify, and troubleshoot STP protocols

Question 434

Which command would you use to see which switch interface is associated with a particular MAC address?

- ☐ show interface mac
- ☐ show mac
- ☒ show mac-address-table
- ☐ show ip interface

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The show mac-address-table command displays a table of every learned MAC address, and the switch port associated with the MAC address. Sample output is as follows:

```
Switch# show mac-address-table
Mac Address Table
-------------------------------------------

Vlan Mac Address Type Ports
---- ----------- ------- -----
1 0040.63d8.ba0a DYNAMIC Fa0/1
1 0004.274c.9ca0 DYNAMIC Fa0/3
1 0040.63d8.bab8 DYNAMIC Fa0/10
1 000f.1fd3.d85a DYNAMIC Fa0/7

Total Mac Addresses for this criterion: 4
```

This output indicates that four MAC addresses have been learned by this switch, and the last column indicates the switch port over which each MAC address was learned, and for which frames destined for each MAC address will be forwarded. The MAC address table is built dynamically by examining the source MAC address of received frames. If the switch receives a MAC address not listed in this table, it will send the frame out all ports except the one from which it was originated.

The show ip interface command is a router command, and displays no information on MAC address tables.

The show interface mac and show mac commands are incorrect because they are not valid Cisco IOS commands.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Licensed to Berend Post berend.post@it-university.nl

Question 435

You recently implemented SNMPv3 to increase the security of your network management system. A partial output of the show run command displays the following output that relates to SNMP:

<output omitted>

snmp-server group TECHS v3 noauth read TECHS write TECHS

Which of the following statements is true of this configuration?

- ☐ It provides encryption, but it does not provide authentication
- ☒ It provides neither authentication nor encryption
- ☐ It provides authentication, but it does not provide encryption
- ☐ It provides both authentication and encryption

Explanation:

Explanation:

It provides neither authentication nor encryption. In SMNPv3, there are three combinations of security that can be used:

noAuthNoPriv- no authentication and no encryption; includes the noauth keyword in the configuration

AuthNoPriv - messages are authenticated but not encrypted; includes the auth keyword in the configuration

AuthPriv - messages are authenticated and encrypted; includes the priv keyword in the configuration

In this case, the keyword noauth in the configuration indicates that no authentication and no encryption are provided. This makes the implementation no more secure than SNMPv1 or SNMPv2.

In SNMPv1 and SNMPv2, authentication is performed using a community string. When you implement SNMP using the noauth keyword, it does not use community strings for authentication. Instead it uses the configured user or group name (in this case TECHS). Regardless, it does not provide either authentication or encryption.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device-monitoring protocols

References:

Licensed to Berend Post berend.post@it-university.nl

SNMP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) > SNMPv3

Question 436

Which of the following are characteristics of Open Shortest Path First (OSPF)? (Choose three.)

- ☐ Administrative distance of OSPF is 90
- ☒ Administrative distance of OSPF is 110
- ☒ OSPF uses the Dijkstra algorithm to calculate the SPF tree
- ☐ OSPF uses the Diffusing Update algorithm (DUAL) algorithm to calculate the SPF tree
- ☐ OSPF uses 224.0.0.5 as multicast address for ALLDRouters
- ☒ OSPF uses 224.0.0.6 as multicast address for ALLDRouters

Explanation:

Explanation:

The following are characteristics of Open Shortest Path First (OSPF) routing protocol:

The default administrative distance is 110.

It uses 224.0.0.6 as the multicast address for ALLDRouters.

It uses the Dijkstra algorithm to calculate the Shortest Path First (SPF) tree.

It uses Internet Protocol (IP) protocol 89.

OSPF supports Non-Broadcast Multi-Access (NBMA) networks such as Frame Relay, X.25, and Asynchronous Transfer Mode (ATM). The default hello interval for NBMA networks is 30 seconds.

OSPF supports point-to-point and point-to-multipoint connections.

It also supports authentication.

OSPF uses 224.0.0.5 as the multicast address for ALLSPFRouters.

It uses link-state updates and SPF calculations that provides fast convergence.

OSPF is recommended for large networks due to good scalability.

It uses cost as the default metric.

There is no maximum hop count as with distance vector routing protocols. The number of hops to a network can be unlimited.

The option stating that AD of OSPF is 90 is incorrect because 90 is the default administrative distance for an internal Enhanced Interior Gateway Routing Protocol (EIGRP) route.

The option stating that OSPF uses the Diffusing Update algorithm (DUAL) algorithm to calculate the SPF tree is incorrect. The DUAL algorithm is used by EIGRP to calculate the SPF tree.

Licensed to Berend Post berend.post@it-university.nl

Keep the following in mind when comparing OSPF and EIGRP:

EIGRP is vendor specific; OSPF is not

EIGRP has an AD of 90; OSPF has an AD of 110

OSPF elects a DR on each multi-access network; EIGRP does not

OSPF uses cost as its metric, and EIGRP uses bandwidth as its metric

The option stating that OSPF uses 224.0.0.5 as multicast address for ALLDRouters is incorrect because OSPF uses 224.0.0.6 as multicast address for ALLDRouters, and 224.0.0.5 as multicast address for ALLSPFRouters.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)

References:

Cisco > Support > IP > IP Routing > Technology Information > Technology White Paper > OSPF Design Guide > Document ID: 7039

Cisco > Support > IP > IP Multicast > Technology Information > Technology Briefs > Internet Protocol IP Multicast Technology

Question 437

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.)

- ☒ Downtime and productivity loss
- ☐ Spread of viruses
- ☒ Revenue loss
- ☒ Information theft
- ☐ Spread of spyware

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A DoS attack can result in network downtime and loss of productivity, revenue loss, and information theft.

A DoS attack is an attack in which legitimate users are denied access to networks, systems, or resources. The potential risks posed by a DoS attack are as follows:

Downtime and productivity loss: A DoS attack causes downtime in the network, which ultimately results in loss of productivity for the organization.

Revenue loss: Organizations that use their Web sites for commerce or vital support services, such as search engines, can incur large revenue losses.

Information theft: DoS attacks can also be aimed at stealing important and confidential information from a network.

Malicious competition: An organization might launch DoS attacks against their competitors to damage their reputation.

A few methods that can help minimize potential risks from DoS attacks are:

Using a firewall, which allows you to block or permit traffic entering into the network, can help to mitigate DoS attacks.

Computers vulnerable to attacks can be shifted to another location or a more secure LAN.

Intrusion Detection Systems (IDS), such as Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS), can be implemented to detect intrusive network or host activity, such as a DoS attack, and raise alerts when any such activity is detected.

A DoS attack does not result in the spread of viruses because viruses are not spread by DoS attacks. Viruses are spread when the network is attacked by a virus or a Trojan horse.

A DoS attack does not result in the spread of spyware. DoS attacks are mainly aimed at exhausting system resources so that legitimate users are denied access to networks, systems, or resources. Spyware is software installed on a computer without the knowledge of the user, and it gathers information about a person or organization. Spyware is generally downloaded through Web sites and e-mail messages.

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot basic device hardening

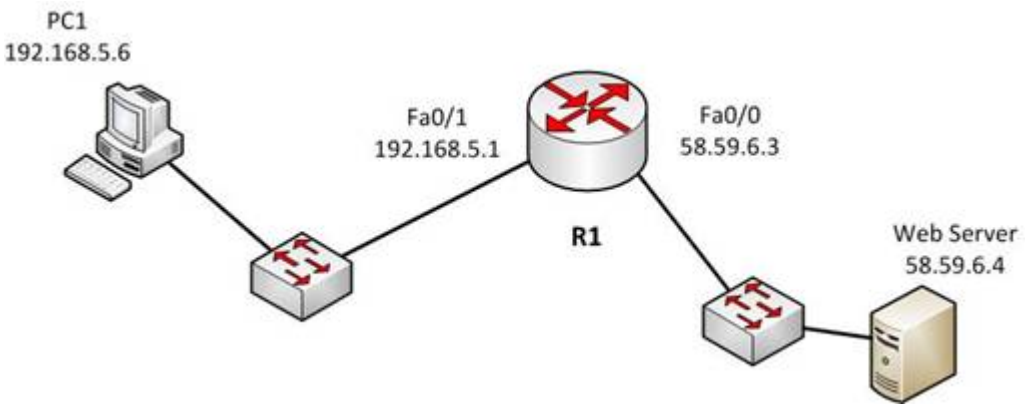
Licensed to Berend Post berend.post@it-university.nl

References:

Cisco > Cisco IOS Security Configuration Guide, Release 12.4 > Traffic Filtering, Firewalls, and Virus Detection > Configuring TCP Intercept (Preventing Denial-of-Service Attacks)

Question 438

Examine the diagram below:



You attempt to make a Telnet connection from PC1 to the switch connected to the Web server, but the connection fails. After making a console connection to the switch connected to the Web server and executing the show run command, you see the following information:

```
<output omitted>

interface vlan 1
ip address 58.59.6.2 255.0.0.0
!
ip default gateway 192.168.5.1
!
line vty 04
password ajax
login
```

Which value is NOT correct?

- ☒ the default gateway
- ☐ the VLAN number
- ☐ the password
- ☐ the login command

Explanation:

Explanation:

The switch is connected to the F0/0/ interface on the router R1. The address of Fa0/0 should be the default gateway for the switch. This means it should be 58.59.6.4 rather than 192.168.5.1.

Licensed to Berend Post berend.post@it-university.nl

The VLAN number is correct. The IP address of a switch is set on the VLAN 1 interface of the switch.

The password can be anything you desire, so that is correct.

The login command is correct. This command instructs the switch to prompt for a password. Since there is a password configured, this will not prevent a connection to the switch.

Objective:

Infrastructure Management

Sub-Objective:

Configure and verify device management

References:

Question 439

You are the network administrator for your company. The network at the company's office is due to be upgraded, and you have been assigned the responsibility of identifying the requirements for designing the network. You need to provide network connectivity to 200 client computers that will reside in the same sub network, and each client computer must be allocated dedicated bandwidth.

Which device should you use to accomplish the task?

- ☐ router
- ☐ hub
- ☒ switch
- ☐ firewall

Explanation:

Explanation:

You should use a switch to accomplish the task in this scenario. A switch is used to provide dedicated bandwidth to each node by eliminating the possibility of collisions on the switch port where the node resides. Switches work at Layer 2 in the Open System Interconnection (OSI) model and perform the function of separating collision domains. When a node resides in its own collision domain, the possibility of collisions (which slow throughput due to the subsequent but necessary retransmission) is eliminated. The advantage of using a switch instead of a hub is that a switch provides dedicated bandwidth to each client, while all connected clients share the bandwidth on a hub.

Licensed to Berend Post berend.post@it-university.nl

A router will not be a suitable device in this scenario. Routers are Network layer devices that are used to separate broadcast domains and connect two or more different subnets or network types. There is only a single subnet in the scenario so a router is not required.

A hub will not be a suitable device in this scenario. Hubs are Physical layer (Layer 1) devices that are used to connect clients to the network. A hub simply broadcasts data to all its ports; it does not create separate collision domains. All clients connected to a hub are a member of a single collision domain. In a scenario where a number of devices connected to a hub are experiencing network slowdowns, especially when using network-based applications, replacing the hub with a switch is almost always the best solution.

A firewall will not be a suitable device in this scenario. A firewall is a device used to secure the network against unauthorized intrusions and malicious attacks.

Objective:

Network Fundamentals

Sub-Objective:

Describe the impact of infrastructure components in an enterprise network

References:

Cisco Documentation > Internetwork Design Guide > Internetworking Design Basics

Question 440

Which of the following is NOT an advantage 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.
- ☒ Static route configuration is more fault tolerant than dynamic routing protocols.

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

Router resources are more efficiently used.

Network security is increased by using static routes.

The following are disadvantages of static routes:

Static routes are not recommended for large networks because static routes are manually configured on the router. Therefore, maintaining routes in a timely manner is nearly impossible.

Static route configuration is not fault tolerant without configuring multiple static routes to each network with varying administrative distances.

All other options are incorrect because these are the advantages of static routes over dynamic routing protocols.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast static routing and dynamic routing

References:

Cisco Documentation > Internetworking Technology Handbook > Routing Basics

Question 441

Which of the following commands will enable a global IPv6 address based on the Modified EUI-64 format interface ID?

- ☐ ipv6 address 5000::2222:1/64
- ☒ ipv6 address autoconfig
- ☐ ipv6 address 2001:db8:2222:7272::72/64 link-local
- ☐ ipv6 enable

Explanation:

Explanation:

To configure the interface to create a global IPv6 address based on the Modified EUI-64 format interface ID, you must enable stateless autoconfiguration. In stateless autoconfiguration, the interface will receive the network prefix from the router advertisement (RA) and generate a full IPv6 address by spreading the 48-bit MAC address of the interface across 64 bits to complete the address. This can all be done simply by executing the ipv6 address autoconfig command at the interface configuration prompt.

 Licensed to Berend Post berend.post@it-university.nl

The command ipv6 address 5000::2222:1/64 is used to manually assign a full IPv6 address to the interface without using stateless autoconfiguration or the eui-64 keyword to manually specify the first 64 bits and allow the last 64 bits to be generated from the MAC address of the interface.

The command ipv6 address 2001:db8:2222:7272::72/64 link local is used to configure a link-local address manually without allowing the system to generate one from the MAC address, which is the default method.

The command ipv6 enable is used to allow the system to generate a link-local address from the MAC address. Because this is the default behavior, the command is not required if any other ipv6 commands have been issued. Regardless of how many manual IPv6 addresses you configure, a link local address is always generated by default.

Objective:

Network Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot IPv6 addressing

References:

Cisco > Product Support > Security > Cisco ASA 5500-X Series Firewalls > Configure > Configuration Guides > Cisco Security Appliance Command Line Configuration Guide, Version 7.2 > Chapter: Configuring IPv6 > Enforcing the Use of Modified EUI-64 Interface IDs in IPv6 Addresses

Cisco > Support > Cisco IOS IPv6 Command Reference > ipv6 address

Licensed to Berend Post berend.post@it-university.nl

Question 442

You are in the process of verifying the operation of your core switches, which are using HSRP. One core switch was left with the default priority; the other was given a lower priority to make it the standby switch. The command show standby brief was executed on one of the switches. Output of the command is shown below:

```
Interface Grp Prio P State  Active Standby       Virtual IP
Vl10      1   90   P Active local  192.168.10.20 192.168.10.1
Vl20      1   90   P Active local  192.168.20.20 192.168.20.1
```

What does this output mean? (Choose all that apply.)

- ☐ this switch is using the default priority
- ☒ this switch is the active HSRP switch
- ☐ the HSRP devices are up and functioning correctly
- ☒ the switch intended to be the active switch has failed and this switch has taken over
- ☒ preemption is enabled for the group

Explanation:

Explanation:

The output in the exhibit indicates that this switch is the active HSRP switch, the switch intended to be the active switch has failed, and that preemption is enabled for the group.

This is the active switch because Active is the State listed for each interface that is a member of HSRP.

The question states that the switch that was intended to be the standby switch was given a priority lower than the default. The default priority is 100, so this is not the switch intended to be the active switch. This information indicates that the switch intended to be the active switch has failed.

Preemption is enabled, as indicated by the P following the priority value in line 2. Since preemption is enabled, the switch with the priority of 100 is still down. When that switch is corrected and joins the group again, it will take over as active.

The HSRP group is still providing access for users, but not all devices are functioning properly.

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

Licensed to Berend Post berend.post@it-university.nl

References:

Cisco IOS Master Command List, Release 12.4T>show ip route profile through sshow mpls atm-ldp summary>Cisco IOS IP Application Services Command Reference>show standby through show udp>show standby

Question 443

Which type of Category 5 unshielded twisted-pair (UTP) cable is used to work as a trunk between two switches?

- ☐ RJ-45 straight-through
- ☐ RJ-41 crossover
- ☐ RJ-11 straight-through
- ☒ RJ-45 crossover

Explanation:

Explanation:

An RJ-45 crossover cable connects two switches. To act as a trunk a trunking protocol such as ISL or 802.1q must be configured on the link. . A trunk is a connection between two switches that is used to carry traffic from multiple VLANs.

In general, the rule to follow when choosing between a straight-through and a crossover cable is:

When connecting like devices (i.e. router to router, switch to switch), use a crossover cable.

When connecting dissimilar devices (i.e. switch to router), use a straight-through cable.

The one exception to this rule is when connecting a computer NIC to a router, in which case a crossover cable is used. Be aware, however, that many devices, including network cards in computers, now have the ability to sense automatically when they are connected to a like device and adapt to the connection, making crossover cables unnecessary in those situations.

You should not choose an RJ-45 straight-through cable. The cable type to be used depends on the circuit connection of the hardware. To connect two switches, a crossover cable is required. The difference between a straight-through cable and a crossover cable lies in the location of the wire termination on the two ends of an RJ-45 cable. If the UTP cable wire connects Pin 1 of one side to Pin 1 of other side and Pin 2 to 2 through all eight pins of the RJ 45 connector, the cable is said to be straight-through. On the other hand, if Pin 1 of one side of an RJ-45 cable connects to Pin 3 of the other end, and Pin 2 connects to Pin 6 of the other end, it is known as a crossover cable. A straight-through cable is used to connect a computer's network interface card (NIC) to a hub or switch.

Licensed to Berend Post berend.post@it-university.nl

You should not choose an RJ-41 crossover cable. RJ-41 is a single-line universal data jack normally associated with fixed-loss loop (FLL) or programmed (P) modems. It is not used between switches.

You should not choose an RJ-11 straight-through cable type. RJ-11 UTP cables have four pins and are used to connect voice instruments. RJ-11 UTP cables are not intended for connecting computers and transferring data. They are commonly used for telephones and modems.

Note: Cisco switches have an auto-mdix feature that notices when the wrong cabling pinouts are used, and readjusts the switch's logic so that the cable will work.

Objective:

Network Fundamentals

Sub-Objective:

Select the appropriate cabling type based on implementation requirements

References:

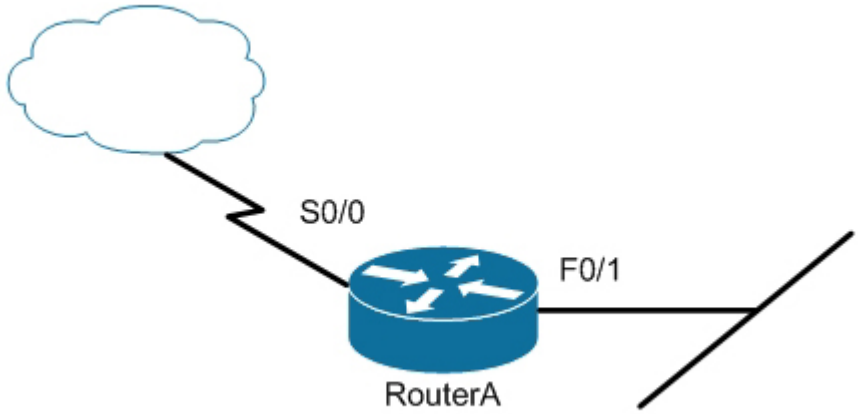
Cisco Documentation > Internetwork Design Guide > Designing Switched LAN Internetworks > Technologies for Building Switched LAN Internetworks

Cisco > Troubleshooting Technotes > Cisco 7000 Series Routers > Cabling Guide for Console and AUX Ports > Types of RJ-45 Cabling

Licensed to Berend Post berend.post@it-university.nl

Question 444

Users on the LAN are unable to access the Internet. How would you correct the immediate problem?



Router# show ip interface brief

Interface IP-Address OK? Method Status Protocol
FastEthernet 0/0 unassigned YES unset down down
FastEthernet 0/1 172.16.1.254 YES NVRAM up up
Serial0/0 200.16.4.25 YES NVRAM administratively down down
Serial0/1 unassigned YES unset down down

- ☐ Configure a bandwidth on the serial interface.
- ☒ Perform a no shutdown command on the serial interface.
- ☐ Configure a private IP address on the Fastethernet0/0 LAN interface.
- ☐ Change the IP address on the serial interface.

Explanation:

Explanation:

The output indicates that the serial interface leading to the Internet is administratively down. All router interfaces are disabled by default due to the presence of a shutdown command in the running configuration. The no shutdown command removes this configuration, and the interface becomes active. The command sequence is:

Router(config)# interface serial0/0

Router(config-if)# no shutdown

Although it was not the problem in the scenario, the S0/0 interface could also cause an error if it is configured as shown in this output:

Licensed to Berend Post berend.post@it-university.nl

Interface IP-Address OK? Method Status Protocol

Serial0/0 200.16.4.25 YES NVRAM up down

In this example, the S0/0 interface has been enabled, and while there is Layer 1 connectivity (the Status column), Layer 2 is not functioning (the Protocol column). There are two possible reasons for this result:

Interface S0/0 is not receiving a clock signal from the CSU/DSU (if one is present).

The encapsulation type configured on S0/0 does not match the type configured on the other end of the link (if the other end is a router).

Configuring a bandwidth on the serial interface is incorrect because the output indicates the interface is administratively down, which does not pertain to bandwidth.

Configuring a private IP address on the Fastethernet0/0 LAN interface is incorrect because the output indicates the problem is with the disabled serial interface.

The IP address on the serial interface may or may not be valid, but it is not the immediate cause of the connectivity problem. The serial interface is disabled.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Troubleshoot interface and cable issues (collisions, errors, duplex, speed)

References:

Cisco > Support > Administrative Commands > shutdown

Licensed to Berend Post berend.post@it-university.nl

Question 445

Which of the following should be a characteristic of the core layer in the Cisco three-layer hierarchical model?

- ☐ redundant components
- ☒ emphasis on high speed
- ☐ PoE
- ☐ QoS

Explanation:

Explanation:

The core layer of the Cisco three-layer hierarchical network design model places an emphasis on high speed. Items such as access control lists (ACLs) and Quality of Service (QoS) should NOT be implemented on this level, as those types of service will slow the high-speed switching process desired at this level.

The three layers of the hierarchical design model are the access layer, the distribution layer, and the core (backbone) layer. The core layer connects to every building block in the modular network, so it must emphasize speed and resilience.

Quality of service and ACLs are implemented on the distribution layer. Layer 3 support is required at this level.

Redundant hardware components and Power over Ethernet (PoE) are characteristics of the access layer. This is the layer where user devices are connected to the network. Layer 2 Port security is also implemented at this layer.

Objective:

Network Fundamentals

Sub-Objective:

Compare and contrast collapsed core and three-tier architectures

References:

Cisco >Home > Solutions > Enterprise > Programs for Enterprise > Design Zone > Design Zone for Campus > Design Guides > Campus Network for High Availability Design Guide > Hierarchical Network Design Model

Licensed to Berend Post berend.post@it-university.nl

Question 446

Which statement is true regarding Inter-Switch Link (ISL) frame tagging?

- ☐ ISL uses a native VLAN.
- ☐ ISL works with non-Cisco switches.
- ☐ ISL adds a 26-byte trailer and 4-byte header.
- ☒ The original Ethernet frame is not modified.

Explanation:

Explanation:

With ISL frame tagging, the original Ethernet frame is not modified. ISL encapsulates the original frame by adding a 26-byte header and a 4-byte Cyclic Redundancy Check (CRC) trailer. The original Ethernet frame is placed between the header and trailer. A normal Ethernet frame can have a maximum size of 1,518 bytes, and therefore adding the header and trailer size gives an ISL frame a maximum size of 1,548 bytes.

ISL frame tagging does not use the concept of a native VLAN. Instead, Institute of Electrical and Electronics Engineers (IEEE) 802.1q frame tagging uses the native VLAN. Unlike ISL trunks, where every frame traversing the trunk is tagged with an ISL header and a trailer, 802.1Q trunks allow untagged frames over the native VLAN. An untagged frame does not carry VLAN identification information in it and is a simple Ethernet frame.

ISL is proprietary to Cisco, and thus does not work with non-Cisco switches.

ISL frame tagging does not add a 26-byte trailer and 4-byte header. It adds a 26-byte header and 4-byte trailer.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Technology Support > LAN Switching > Virtual LANs/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format > Document ID: 17056

Licensed to Berend Post berend.post@it-university.nl

Question 447

Which VLAN can NOT be filtered through the VLAN Trunking Protocol (VTP) Pruning feature of Cisco switches?

- ☒ VLAN 1
- ☐ VLAN 10
- ☐ VLAN 100
- ☐ VLAN 1000

Explanation:

Explanation:

VLAN 1 traffic cannot be pruned. Cisco recommends that VLAN 1 be used for management of VLANs.

VTP pruning is a Cisco VTP feature that allows switches to dynamically delete or add VLANs to a trunk for traffic transmission. It creates an efficient switching network by optimal use of available trunk bandwidth.

The options 10, 100, and 1000 are incorrect because these VLAN numbers can be pruned. By default, VLANs 2 to 1000 are eligible for pruning.

Objective:

LAN Switching Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches

References:

Cisco Press Home > Articles > Cisco Certification > CCNA > CCNA Self-Study (ICND Exam): Extending Switched Networks with Virtual LANs

Licensed to Berend Post berend.post@it-university.nl

Question 448

You are the network administrator for your company. Your company has opened a new site in London. The Chief Technical Officer (CTO) of the company wants to implement a routing protocol that can provide the following features:
Supports multiple large networks
Does not require a hierarchical physical topology
Supports VLSM
Provides loop prevention and fast convergence
Provides load balancing over un-equal cost links

Which routing protocol should be implemented in the new site?

- ☒ Enhanced Interior Gateway Routing Protocol (EIGRP)
- ☐ Open Shortest Path First (OSPF)
- ☐ Interior Gateway Routing Protocol (IGRP)
- ☐ Routing Information Protocol version 2 (RIPv2)

Explanation:

Explanation:

Enhanced Interior Gateway Routing Protocol (EIGRP) is the routing protocol that should be implemented for this scenario. EIGRP is a classless protocol that allows the use of variable length subnet masks (VLSM) and classless interdomain routing (CIDR) for the allocation of IP addresses. The following are characteristics of EIGRP:

Supports large networks due to high scalability.

Does not require a hierarchical physical topology.

Provides loop prevention and fast convergence by using Diffusing Update Algorithm (DUAL).

Performs equal cost load balancing by default.

Can be configured to perform unequal-cost load balancing.

Supports VLSM and CIDR.

Is a hybrid routing protocol (a distance-vector protocol that also provides link-state protocol characteristics).

Is a classless protocol.

Sends partial route updates only when there are changes.

Supports Message-Digest algorithm 5 (MD5) authentication.

Has an administrative distance is 90 for EIGRP internal routes, 170 for EIGRP external routes, and 5 for EIGRP summary routes.

Is only used with Cisco platforms.

All the other options are incorrect because they would not provide the features required in this scenario.

Licensed to Berend Post berend.post@it-university.nl

OSPF requires a hierarchical physical topology.

IGRP does not support VLSM.

RIPV2 is not designed for multiple large networks.

Objective:

Routing Fundamentals

Sub-Objective:

Compare and contrast distance vector and link-state routing protocols

References:

Cisco > Articles > Cisco Certification > CCNP > Shooting Trouble with IP

Cisco > Support > IP > IP Routing > Design > Design TechNotes > Introduction to EIGRP > Document ID: 13669

Question 449

The conference room has a switch port available for use by the presenter during classes. You would like to prevent that port from hosting a hub or switch.

Which of the following commands could be used to prevent that port from hosting a hub or switch?

- ☐ switchport port-security maximum
- ☐ switchport port-security mac address sticky
- ☐ switchport port-security mac address
- ☒ switchport port-security

Explanation:

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.

Licensed to Berend Post berend.post@it-university.nl

The switchport port-security mac address sticky command would not prevent that port from hosting a hub or switch. This command is used to allow a port to dynamically learn the first MAC address it sees in the port, add it to the MAC address table and save it to the running configuration of the switch.

The switchport port-security mac address command would not prevent that port from hosting a hub or switch. This command is used to manually assign a MAC address to a port as a secure address. When used in combination with the switchport port-security maximum command, the use of the port can not only be limited to one address at a time, but also limited to only a specific address. For example, the following set of commands would assure that only the device with the MAC address of 0018.cd33.46b3 will be able to connect to the port:

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security mac-address 0018.cd33.46b3

Objective:

Infrastructure Security

Sub-Objective:

Configure, verify, and troubleshoot port security

References:

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA>Configuring Port Security

Question 450

Which of the following statements is TRUE about trunk ports?

- ☐ A trunk port connects an end-user workstation to a switch.
- ☒ A trunk port uses 802.1q to identify traffic from different VLANs.
- ☐ A trunk port supports a single VLAN.
- ☐ A trunk port uses a straight-through Ethernet cable when connecting two switches.

Explanation:

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

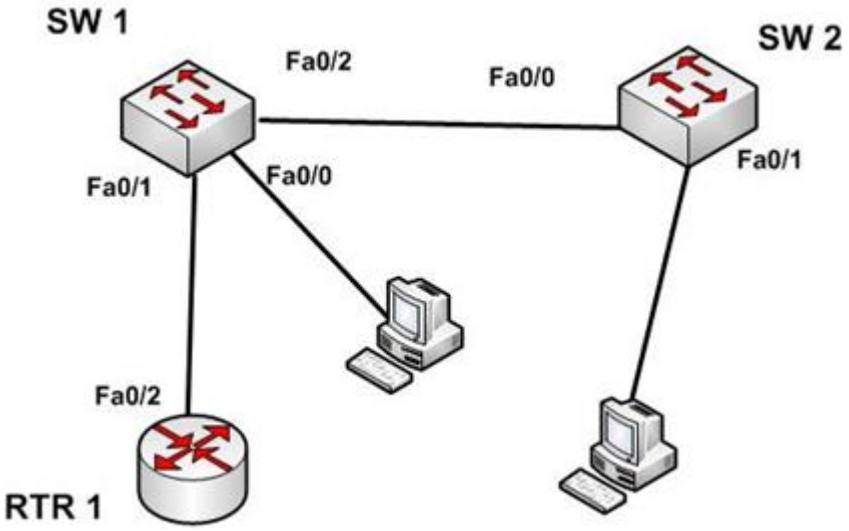
 Licensed to Berend Post berend.post@it-university.nl

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.

Licensed to Berend Post berend.post@it-university.nl

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:

Home > Articles > Network Technology > General Networking > VLANs and Trunking

Question 451

What is the HSRP virtual router MAC address for the virtual router for HSRP group 31?

- ☒ 0000.0c07.ac1f
- ☐ ac1f
- ☐ 0c07
- ☐ 07.ac

Explanation:

Explanation:

The Hot Standby Router Protocol (HSRP) virtual MAC address for the virtual router for HSRP group 31 is 0000.0c07.ac1f. A Media Access Control (MAC) address is a 6-byte value that is unique for every networked device. MAC addresses are typically written in hexadecimal notation. The address 0000.0c07.ac1f is a MAC address for an HSRP virtual router; this address can also be written as 00-00-0c-07-ac-1f or 00.00.0c.07.ac.1f. Hexadecimal letters can be written as either lowercase or uppercase letters.

The MAC address for an HSRP virtual router consists of the vendor ID, the HSRP code and the group ID. The vendor ID corresponds to the first three bytes of the MAC address. A vendor ID of 0000.0c indicates that the device was manufactured by Cisco. The HSRP code corresponds to the fourth and fifth bytes of the MAC address. The HSRP code for a virtual router is always equal to 07.ac. Finally, the group ID corresponds to the last byte of the MAC address. For example, a group ID of 1f, when converted to decimal, indicates that the virtual router belongs to HSRP group 31.

Licensed to Berend Post berend.post@it-university.nl

Objective:

Infrastructure Services

Sub-Objective:

Configure, verify, and troubleshoot basic HSRP

References:

Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing

Question 452

Which Cisco Internetwork Operating System (IOS) command is used to view the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets that are sent and received?

- ☐ show eigrp neighbors
- ☐ show ip eigrp interfaces
- ☐ show ip eigrp packets
- ☒ show ip eigrp traffic
- ☐ show ip route
- ☐ show ip eigrp topology

Explanation:

Explanation:

The show ip eigrp traffic command is used to view the number of EIGRP packets that are sent and received. The syntax of the command is:

Router# show ip eigrp traffic [autonomous-system-number]

The autonomous-system-number parameter is optional. The output of the command is as follows:

Router# show ip eigrp traffic

IP-EIGRP Traffic Statistics for process 78

Hellos sent/received: 2180/2005

Updates sent/received: 70/21

Queries sent/received: 3/1

Replies sent/received: 0/3

Acks sent/received: 22/11

Licensed to Berend Post berend.post@it-university.nl

The show ip eigrp neighbors command is incorrect because it does not show the number of packets sent or received. It does show IP addresses of the devices with which the router has established an adjacency, as well as the retransmit interval and the queue count for each neighbor, as shown below:

Router# show ip eigrp neighbors

IP-EIGRP Neighbors for process 49

Address Interface Holdtime Uptime Q Seq SRTT RTO

(secs) (h:m:s) Count Num (ms) (ms)

146.89.81.28 Ethernet1 13 0:00:41 0 11 4 20

146.89.80.28 Ethernet0 12 0:02:01 0 10 12 24

146.89.80.31 Ethernet0 11 0:02:02 0 4 5 20

The show ip eigrp interfaces command is incorrect because this command is used to view information about the interfaces configured for EIGRP.

The show ip eigrp packets command is incorrect because it is not a valid Cisco IOS commands.

The show ip route command will not display EIGRP packets that are sent and received. It is used to view the routing table. When connectivity problems occur between subnets, this is the logical first command to execute. Routers must have routes to successfully send packets to remote subnets. Using this command is especially relevant when the underlying physical connection to the remote network has been verified as functional, but routing is still not occurring.

The show ip eigrp topology command is incorrect because it does not show the number of packets sent or received. This command displays all successor and feasible successor routes (if they exist) to each network. If you are interested in that information for only a specific destination network, you can specify that as shown in the output below. When you do, the command output displays all possible routes, including those that are not feasible successors:

Licensed to Berend Post berend.post@it-university.nl

```
Router# show ip eigrp topology 25.0.0.5 255.255.255.255

IP-EIGRP topology entry for 25.0.0.5/32 State is Passive, Query
origin flag is 1, 1 Successor(s), FD is 41152000

<output omitted>

10.1.0.1 (serial0), from 10.1.0.1 composite
metric is 46152000/41640000
<output omitted>
10.0.0.2 (serial0.1), from 10.0.0.2
composite metric is 53973240/120256
<output omitted>
10.1.0.3 (serial0), from 10.1.0.3
composite metric is 46866176/46354176
<output omitted>
10.1.1.1 (serial0.1), from 10.1.1.1
composite metric is 46670776/46251776
<output omitted>
```

In the above output, four routers are providing a route to the network specified in the command. However, only one of the submitted routes satisfies the feasibility test. This test dictates that to be a feasible successor, the advertised distance of the route must be less than the feasible distance of the current successor route.

The current successor route has a FD of 41152000, as shown in the first section of the output. In the values listed for each of the four submitted routes, the first number is the feasible distance and the second is the advertised distance. Only the route received from 10.0.0.2 (second section) with FD/AD values of 53973240/120256 satisfies this requirement, and thus this route is the only feasible successor route present in the topology table for the network specified in the command.

Objective:

Routing Fundamentals

Sub-Objective:

Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)

References:

Cisco > Cisco IOS IP Routing Protocols Command Reference > Routing Information Protocol Commands > show ip eigrp traffic

Licensed to Berend Post berend.post@it-university.nl

Question 453

Based on the output of the show mac-address-table command shown below, where will the switch that produced this output send a frame with a destination MAC address of ffff.ffff.ffff?

Vlan Mac address Type Ports
<output omitted>
1 000f.e544.c2b3 dynamic Fa0/10
1 000d.4589.00b8 dynamic Fa0/5
1 00bd.000b.005bb dynamic Fa0/8
1 0001.0d44.bbdb dynamic Fa0/12
1 0014.0bd4.0054 dynamic Fa0/15
1 00bb.224b.0ac5 dynamic Fa0/1

- ☒ to all ports, listed and unlisted, except the originating port
- ☐ to Fa0/10, Fa0/5, Fa0/8, Fa0/12, Fa0/15, and Fa0/1
- ☐ to no ports, since the MAC address isn't in the table
- ☐ to all ports excluding the ports listed in the table
- ☐ to port Fa0/15

Explanation:

Explanation:

The MAC address ffff.ffff.ffff is called the Layer 2 broadcast address. It will be sent to all ports listed in the table, or known to the switch, as well as to all those unlisted, or not yet known by the switch. This excludes the originating port only.

It will not send the frame only to the ports listed in the table (Fa0/10, Fa0/5, Fa0/8, Fa0/12, Fa0/15, and Fa0/1). It will also be sent to ports that are as yet unknown by the switch.

It will not prevent the frame from being sent to any ports because the MAC address is not listed. Broadcast addresses are not listed in the MAC address table. These addresses are only used to send to all hosts.

It will not send the frame to all ports except the ports listed. This would be the switch's behavior if the address of the frame in question was not a broadcast address and was not listed in the MAC address table. Until a switch knows where a frame goes, it will send the frame to all ports that are still unknown or unlisted, with the exception of the port on which it arrived.

It will not send the frame to port Fa0/15 only. If the frame were addressed to 0014.0bd4.0054, the switch would forward the frame to that port only. When a switch receives a unicast frame with a destination MAC address that is listed in the table, it will only send the frame to that port.

Objective:

 Licensed to Berend Post berend.post@it-university.nl

LAN Switching Fundamentals

Sub-Objective:

Describe and verify switching concepts

References:

Cisco > Internetworking Technology Handbook > Bridging Basics > Bridging and Switching Basics

Question 454

You receive the following error message after addressing and enabling an interface:

%192.168.16.0 overlaps with FastEthernet0/0

Which two are NOT the causes of the error message? (Choose two.)

- ☐ incorrect subnet mask in the new interface
- ☐ incorrect IP address on the new interface
- ☒ incorrect encapsulation configured
- ☒ failure to issue the no shutdown command

Explanation:

Explanation:

The error message %192.168.16.0 overlaps with FastEthernet0/0 indicates that the newly configured interface is in the same subnet as an existing interface. This can occur if there is an incorrect subnet mask or an address that inadvertently places the new interface in that subnet. Each router interface must be in a different subnet to function. For example, when the series of commands below is executed on a router, it will elicit the error message because the two IP addresses used are in the same subnet given the subnet mask in use.

Router#config t

Router(config)#interface S0

Router(config-if)#ip address 192.168.1.17 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)interface S1

Router(config-if)#ip address 192.168.1.65 255.255.255.0

Router(config-if)#no shutdown

0%192.168.1.0 overlaps with Serial 0

Licensed to Berend Post berend.post@it-university.nl

It's also a valuable skill to be able to recognize these problems before the router tells you about them. In the diagram below, you should be able to spot the problem with the two planned addresses on the router as being in the same subnet before you receive the error message.

An incorrect encapsulation would prevent the interface from working, but would not generate this message.

If the no shutdown command had not been issued, we would not be receiving this error. It is only generated when an attempt is made to enable an incorrectly configured interface.

Objective:

Routing Fundamentals

Sub-Objective:

Troubleshoot basic Layer 3 end-to-end connectivity issues

References:

Cisco Documentation > Configuring IP Addressing

Licensed to Berend Post berend.post@it-university.nl

Question 455

Based on the command output below, which of the interfaces on Router1 are trunk ports?

```
Router1# show mac-address-table

Dynamic Addresses Count: 14
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count: 23
Total MAC addresses: 33
Non-static Address Table:
Destination Address Address Type VLAN Destination Port

------------------- ------------ ---- --------------------

0010.0de0.e289 Dynamic 1 FastEthernet0/1
0010.7b00.1540 Dynamic 1 FastEthernet0/5
0010.7b00.1545 Dynamic 1 FastEthernet0/5
0060.5cf4.0076 Dynamic 3 FastEthernet0/1
0060.5cf4.0077 Dynamic 3 FastEthernet0/1
0060.5cf4.1315 Dynamic 2 FastEthernet0/1
0060.70cb.f301 Dynamic 1 FastEthernet0/2
00e0.1e42.9978 Dynamic 1 FastEthernet0/3

<output omitted>
```

- ☒ Fa0/1
- ☐ Fa0/2
- ☐ Fa0/3
- ☐ Fa0/5

Explanation:

Explanation:

Interface Fa0/1 is a trunk port. The output shows that it has MAC addresses that belong to VLANs 1, 2 and 3. Only trunk ports can carry traffic from multiple VLANs.

Fa0/2 is not a trunk port. It only carries traffic from VLAN 1.

Fa0/3 is not a trunk port. It only carries traffic from VLAN 1.

Fa0/5 is not a trunk port. It only carries traffic from VLAN 1.

Objective:

Infrastructure Management

Sub-Objective:

Licensed to Berend Post berend.post@it-university.nl

Use Cisco IOS tools to troubleshoot and resolve problems

References:

Licensed to Berend Post berend.post@it-university.nl