Exam : 642-811

Title : Building Cisco Multilayer Switched Networks (BCMSN)

Ver : 10-01-07

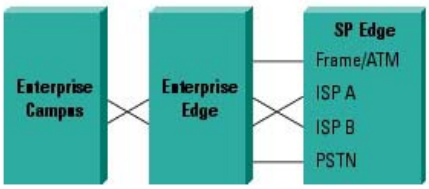
QUESTION 1:

In the Enterprise Composite Network Model; what are three of the functional areas? (Choose three)

A. Enterprise Campus
B. Enterprise Edge
C. Service Provider Edge
D. Building Access
E. Server Farm
F. Campus Backbone
G. Wiring Closet

Answer: A, B, C

Explanation:
Although most enterprise networks have evolved with growing IT requirements, the Cisco SAFE architecture uses a modular approach, which has two main advantages. First, it allows the architecture to address the security relationship between the various functional blocks of the network. Second, it permits designers to evaluate and implement security on a module-by-module basis, instead of attempting the complete architecture in a single phase.
The following figure illustrates the first layer of modularity in SAFE. Each block represents a functional area. The Internet service provider (ISP) module is not implemented by the enterprise, but is included to the extent that specific security features should be requested of an ISP in order to mitigate against certain attacks.



This figure illustrates the three functional areas of the Network model: The enterprise campus, enterprise edge, and the service provider edge.
Reference:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009

QUESTION 2:

The Certkiller network is upgrading all switches to be layer 3 capable. What are some of the advantages experienced with layer 3 switching (Select all that apply)?

A. High-performance packet switching
B. Security
C. Flow accounting

D. Low latency
E. Low per-port cost
F. Quality of service
G. Increased Scalability
H. Hardware-based packet forwarding

Answer: A, B, C, D, E, F, G, H

Explanation:
Traditional software-based routers are simply not fast enough to do the job. Layer 3 switching is primarily a routing solution implemented in the switch's fabric. Instead of using traditional software-based routers, savvy switch manufacturers are integrating router functionality into their switch hardware, offering faster, more secure, more reliable routing solutions
The advantages are clear. Layer 3 switching provides hardware-based routing at wire speeds, which significantly improves overall performance. Routing packets via hardware eliminates bottlenecks associated with software-based routers and delivers seamless implementation into existing networks.
Providing this boost in performance and removing LAN router bottlenecks, switched networks more efficiently utilize available bandwidth. Users get a responsive, high-speed network that is more stable and reliable while protecting the existing investment in their network infrastructure. Layer 3 switches are usually managed, allowing network managers to effortlessly configure and manage the routing process. Reduced support costs make this a true cost-effective solution with the added benefits of higher network reliability and a quicker response time

---

QUESTION 3:

Which statement correctly describes the extended system ID?

A. It is the 2-bit number of the MSTP instance.
B. It is the VLAN identifier value and allows for 4096 BIDs to be uniquely identified.
C. It is the bridge MAC address which is allocated from a pool of MAC addresses that are factory assigned.
D. It is a hex number used to measure the preference of a bridge in the spanning-tree algorithm.
E. None of the above

Answer: B

Explanation:
Each VLAN on each network device has a unique 64-bit bridge ID consisting of a bridge priority value, an extended system ID, and an STP MAC address allocation.
Extended system IDs are VLAN IDs between 1025 and 4096. Cisco Switches support a 12-bit extended system ID field as part of the bridge ID. Chassis that support only 64 MAC addresses always use the 12-bit extended system ID. On chassis that support 1024

MAC addresses, you can enable use of the extended system ID. STP uses the VLAN ID as the extended system ID.
Through the use of the extended system ID, up to 4096 VLANS can be used instead of the 1024 that are used as the default.

QUESTION 4:

A new Certkiller branch is being opened and you are contemplating the use of Unshielded Twisted Pair (UTP) cable for this new office. What is the maximum distance that can be used between two nodes on this UTP network?

A. 100 meters
B. 150 meters
C. 100 feet
D. 2 kilometers
E. 300 meters
F. None of the above

Answer: A

Explanation:
UTP cabling does not offer as high bandwidth or as good protection from interference as coaxial or fiber optic cables, but it is less expensive and easier to work with. The maximum length for an unshielded twisted pair (UTP) cable segment is 100 meters

---

QUESTION 5:

A new Certkiller branch office is being installed and connected, with individual stations and servers being plugged in to the LAN switch. What kind of cable should be used to connect a router, server, or individual workstation to a switch?

A. rollover cable
B. crossover cable
C. straight-through cable
D. coax cable

Answer: C

Explanation:
To connect any end device to a switch you have to use a straight cable.
Incorrect Answers:
A: A rollover cable is used to connect to the console port of a switch or a router.
B: Crossover cables are used to connect: two computers directly together, two hubs, a hub to a switch, a cable modem to a router, or two router interfaces together. It is also used for directly connecting a PC into a router's Ethernet port.

D: Coaxial cable is typically used for DS3 interfaces. It is not normally used in switched LAN networks.

QUESTION 6:

Gigabit Ethernet switches are being installed throughout the Certkiller network. Which of the following cable types are appropriate for Gigabit Ethernet applications? (Select two)

A. Cat-3 UTP
B. Cat-5 UTP
C. RG-58 coax
D. 50 micron MMF
E. 62.5 micron SMF

Answer: B, D

Explanation:
The following lists the Gigabit Ethernet Cabling options, along with their respective Distance Limitations:
1000BASE-T EIA/TIA Category 5 UTP 4 100 m
1000BASE-SX Multimode fiber (MMF) with 62.5 micron core; 850 nm laser 1 275 m
MMF with 50 micron core; 850 nm laser 1 550 m
1000BASE-LX/LH MMF with 62.5 micron core; 1300 laser 1 550 m
Signal-mode fiber (SMF) with 50 micron core;
1300 nm laser
1 550 m
B: 1000BaseT use category 5 UTP.
D: 1000BaseSX use 62.5 and 50-micron MMF

QUESTION 7:

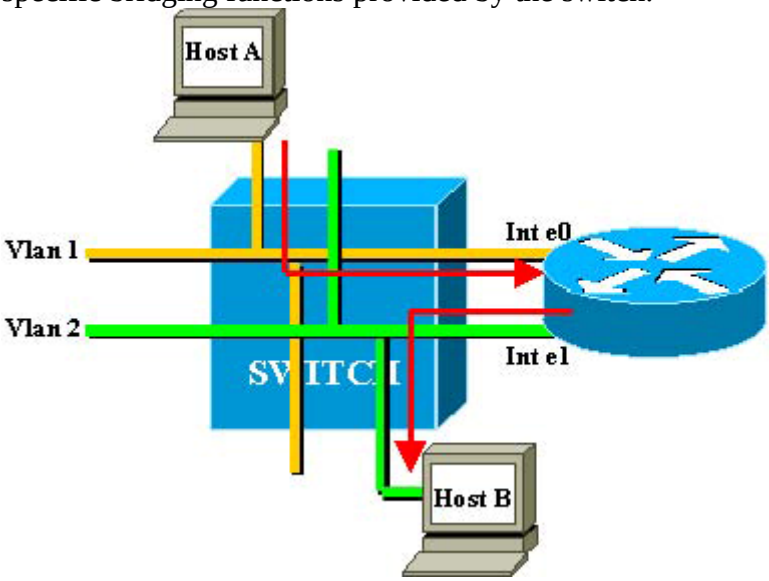
You need to ensure full connectivity exists between all stations on the Certkiller LAN. By what means could you provide a Layer 3 data path between two separate VLANs? (Choose two)

A. A VLAN trunking
B. An external router
C. An internal processor
D. VLAN capable bridge
E. EtherChannel

Answer: B, C

Explanation:

The only connectivity that we want between VLANs is achieved at Layer 3 (L3) by a router. This is Inter-VLAN routing. To further simplify the diagrams, we will represent VLANs as different physical Ethernet segments, as we are not really interested in the specific bridging functions provided by the switch.



In the above diagram, the two VLANs are considered as two different Ethernet segments. Inter-VLAN traffic needs to go through the external router. If host A wants to communicate with host B, it will typically use the router as a default gateway.
In order to provide connectivity between VLANs, traffic must be routed. This can be either achieved via an external router, or an internal route processor such as the Route Switch Module (RSM) found in Cisco Catalyst 6500 switches.

QUESTION 8:

Which layer 3 switching method utilizes a forwarding information base (FIB)?

A. Route caching
B. Demand-based switching
C. Flow-based switching
D. Topology-based switching

Answer: D

Explanation:
Cisco Express Forwarding (CEF) is an example of a topology-based switching mechanism that uses a FIB. CEF provides a topology-based switching mechanism that switches packets at hundreds of millions of packets per second, while maintaining high-speed services.
In a non-Cisco Express Forwarding implementation, the first packet of any flow needs to be processed by the CPU. This can lead to decreased performance, particularly if many new flows are being set up. In a Cisco Express Forwarding-based switch, the forwarding table is prepopulated based on the routing table. This helps to ensure both predictability

in the event of a route flap and that CPU overload will not affect performance. All Cisco Catalyst switching products support Cisco Express Forwarding today.
Cisco Express Forwarding (CEF) switching is a proprietary form of scalable switching intended to tackle the problems associated with demand caching. With CEF switching, the information which is conventionally stored in a route cache is split up over several data structures. The data structures that provide optimized lookup for efficient packet forwarding include:
1. The Forwarding Information Base (FIB) table - CEF uses a FIB to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and these changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. This table is used in this topology based switching method.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 412.

QUESTION 9:

New access layer switches are being installed in the 3-tiered Certkiller network.
Which of the attributes below correctly describe the characteristics of access layer switches? (Choose all that apply.)

A. High port density to connect to end users.
B. Robust Layer 3 routing throughput
C. Inter-VLAN routing
D. Low cost
E. Security
F. None of the above

Answer: A, D

Explanation:
The Access Layer:
The main criteria for access devices are to provide this functionality with low-cost, high port density devices. Access layer switches should provide connections for as many end devices as possible, as fast as possible.
Incorrect Answers:
B, C: Layer 3 (Inter VLAN) routing is processor intensive and should generally be used only in larger, more expensive distribution layer switches instead of at the access layer.
E: The use of security features such as access lists should be used at the distribution layer of the network.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 21

QUESTION 10:

In an effort to reduce the number of broadcast traffic within the Certkiller network,

new Catalyst switches are being installed. Which of the following statements correctly describe Layer 2 broadcast traffic?

A. Layer 2 broadcast traffic is blocked by Layer 3 devices.
B. A new packet is sent each time the client requests it.
C. Each frame uses a special address for which only interested clients listen.
D. It is the most efficient way to send data to a small group of clients.
E. Each packet is refreshed when requested.

Answer: A

Explanation:
LAN broadcasts do not cross routers (Layer 3 devices). By default, routers do not forward any broadcast packets, unless the "IP helper-address" command is configured.
Incorrect Answers:
B: Each broadcast is only send once.
C: Multicast is more efficient. Broadcast reach all clients, multicast will only reach the member of the multicast group.
D: All clients on the subnet receive the broadcast traffic.
E: Broadcast traffic is not refreshed or resent. Doing so could result in a broadcast storm.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 17.

QUESTION 11:

The Certkiller network is upgrading the network to use switches that are capable of multilayer switching. Which statement below best describes the concept of multilayer switching (MLS)?

A. Switches that operate at the access, distribution, and core layer at the design model.
B. An OSI Layer 1 and 2 bridging technique.
C. A technique to provide hardware switching of Layer 3 unicast packets.
D. A flow-based Layer 3 packet routing methodology.

Answer: C

Explanation:
Switches are layer two devices originally developed to contain broadcasts. A multilayer switch is an improvement because it contains extra processing power to consider layer 3 address information, so it effectively works at more than one layer.
Multi-Layer Switching (MLS) has become a highly desired method of accelerating routing performance through the use of dedicated Application Specific Integrated Circuits (ASICs). Traditional routing is done through a central CPU and software. MLS offloads a significant portion of routing (packet rewrite) to hardware, and thus has also been termed switching. MLS and Layer 3 switching are equivalent terms.

QUESTION 12:

Which two table types are CEF components? Select two.

A. forwarding information base
B. adjacency tables
C. neighbor tables
D. caching tables
E. route tables.

Answer: A, B

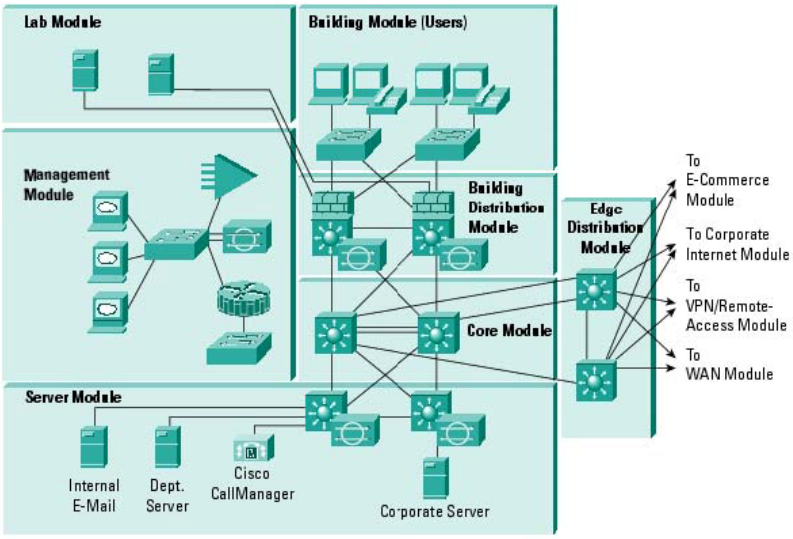
QUESTION 13:

In the Enterprise Composite Model, what are the four major modules of the Campus functional area? (Choose four)

A. Campus Infrastructure
B. Network Management
C. Server Farm
D. Edge Distribution (Enterprise Edge)
E. Access Distribution
F. Core Layer

Answer: B, C, D, F

Explanation:
Following is a detailed analysis of all of the modules contained within the enterprise campus. The following figure shows thiscampus:
Enterprise Campus Detail



Management Module

The primary goal of the management module is to facilitate the secure management of all devices and hosts within the enterprise architecture.
Core Module
The core module in the network architecture is nearly identical to the core module of any other network architecture. It merely routes and switches traffic as fast as possible from one network to another.
Building Distribution Module
This module provides distribution layer services to the building switches. These include routing, quality of service (QoS), and access control. Requests for data flow into these switches and onto the core, and responses follow the identical path in reverse.
Building Access Module
This module is described as the extensive network portion that contains end-user workstations, phones, and their associated Layer 2 access points. Its primary goal is to provide services to end users.
Server Module
The server module's primary goal is to provide application services to end users and devices. Traffic flows on the server module are inspected by on-board intrusion detection within the Layer 3 switches.
Edge Distribution Module
This module aggregates the connectivity from the various elements at the edge. Traffic is filtered and routed from the edge modules and routed into the core.
Incorrect Answers:
A: This is incorrect because 'Campus Infrastructure' refers to the collective of all network equipment on the campus.
E: This is incorrect because the 'Access Distribution' area is not a defined area, it is just a combination of the already familiar terms 'access' (from the OSI access layer) and 'distribution' (from this models Edge Distribution).

QUESTION 14:

The Certkiller network is a large campus network. Which of the following layers are typically found on this type of campus network? (Select all that apply)

A. Access
B. Front
C. Distribution
D. Back
E. Core

Answer: A, C, E

Explanation:
An enterprise campus network can be broken down to small, medium, and large locations. In most instances large campus locations will have a three-tier design with a wiring closet component (Ethernet access layer), a distribution layer, and core layer. Small campus locations will likely have a two-tier design with wiring closet component

(Ethernet access layer) and a backbone core (collapsed core and distribution layers). Medium-sized campus network designs will sometimes use a three-tier implementation or a two-tier implementation depending on the number of ports, service requirements, manageability, performance, and availability levels that are required.

QUESTION 15:

You are troubleshooting a problem between two workstations (CK1 & CK2). Workstation CK1 is unable to ping workstation CK2 . They are both connected to the same switch, the same VLAN, and to they're both in the same subnets. What should you do to verify connectivity? (Select two)

A. Verify that the router for the VLAN is operational.
B. Check the speed and duplex settings.
C. Check both devices for proper default gateway settings.
D. Check to see if the MAC addresses are in the CAM table.

Answer: B, D

Explanation:
Because the two workstations are physically connected to the same switch (which isn't necessarily required to be in the same VLAN), you can rule out the possibility of a compromised physical layer connection. If the speed and duplex settings on each device are mismatched then there could indeed be connectivity issues so B is correct. If for whatever reason the MAC address for CK2 isn't on the switches CAM table then the switch won't know the whereabouts of CK2 making the ping ineffective.
Incorrect Answers:
A: Since the two switches are the on same VLAN there is no need to check the router, so A is incorrect.
C: Since the two switches are both in the same subnet and the same VLAN the default gateway settings wouldn't be an issue, so C is incorrect.

QUESTION 16:

The Certkiller LAN switches are being configured to support the use of Dynamic VLANs. Which of the following are true of dynamic VLAN membership? (Select all that apply)

A. VLAN membership of a user always remains the same even when he/she is moved to another location.
B. VLAN membership of a user always changes when he/she is moved to another location.
C. Membership can be static or dynamic.
D. Membership can be static only.
E. None of the above.

Answer: A, C

Explanation:
Dynamic VLAN memberships are based on the users MAC address connected to the port. If you have VTP server, a VTP database file, a VTP client switch, and a dynamic port; regardless of where your physical location is, you can still remain in the same VLAN.
Incorrect Answers:
B: This was true before the use of Dynamic VLAN membership, as VLANs were assigned to ports, not users.
D: VLAN memberships can be either static or dynamic.

QUESTION 17:

The Certkiller LAN switches are being configured to support the use of Dynamic VLANs. What should be considered when implementing a dynamic VLAN solution? (Select two)

A. Each switch port is assigned to a specific VLAN.
B. Dynamic VLANs require a VLAN Membership Policy Server.
C. Devices are in the same VLAN regardless of which port they attach to.
D. Dynamic VLAN assignments are made through the command line interface.

Answer: B, C

Explanation:
With VLAN Membership Policy Server (VMPS), you can assign switch ports to VLANs dynamically, based on the source Media Access Control (MAC) address of the device connected to the port. When you move a host from a port on one switch in the network to a port on another switch in the network, the switch assigns the new port to the proper VLAN for that host dynamically.
Note: There are two types of VLAN port configurations: static and dynamic.
Incorrect Answers
A: In a static VLAN, the administrator assigns switch ports to the VLAN, and the association does not change until the administrator changes the port assignment. However, this is not the case of dynamic VLANs.
D: The Command Line Interface is not used for dynamic VLAN assignments.
Reference: Cisco Online, Configuring Dynamic Port VLAN Membership with VMPS

QUESTION 18:

What is the preferred method of filtering bridged traffic within a VLAN?

A. Ethernet maps
B. Router ACLs
C. VLAN access maps
D. IP ACLs

Answer: C

Explanation:
VLAN ACLs or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN.
Each VLAN access map can consist of one or more map sequences, each sequence with a match clause and an action clause. The match clause specifies IP, IPX, or MAC ACLs for traffic filtering and the action clause specifies the action to be taken when a match occurs. When a flow matches a permit ACL entry, the associated action is taken and the flow is not checked against the remaining sequences. When a flow matches a deny ACL entry, it will be checked against the next ACL in the same sequence or the next sequence. If a flow does not match any ACL entry and at least one ACL is configured for that packet type, the packet is denied.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080160

QUESTION 19:

You are assigning VLANs to the ports of switch CK1 . What VLAN number value is an assigned to the default VLAN?

A. VLAN 1003
B. VLAN 1
C. VLAN ON
D. VLAN A
E. VLAN 0

Answer: B

Explanation: The default VLAN is VLAN 1. Although this VLAN can be modified, it can not be deleted from the switch. The following VLANs are on by default for all Cisco Catalyst switches:
VLAN 1 - Default VLAN
VLAN 1002 - Default FDDI VLAN
VLAN 1003 - Default Token Ring VLAN
VLAN 1004 - Default FDDI Net VLAN
VLAN 1005 - Default Token Ring Net VLAN
Incorrect Answers:
A: This is the default Token Ring VLAN that is installed in the switch IOS. It is seldom used.
C: ON is a VTP configuration mode, but is not a normal VLAN name.
D: Although any VLAN can be named VLAN A, it is not created by default.
E: Although in Cisco IOS the number 0 has significance (i.e. ethernet 0, console port 0, serial 0) in VLANs 1 is the default. VLAN 0 is an invalid VLAN and can not be used.

QUESTION 20:

The VLANs in switch CK1 are being modified. Which of the following are updated in CK1 every time a VLAN is modified? (Select all that apply)

A. Configuration revision number
B. Configuration revision flag field
C. Configuration revision reset switch
D. Configuration revision database
E. None of the above.

Answer: A, D

Explanation:
For accountability reasons, every time a VLAN is modified the revision number changes, as does the information in the configuration revision database (as that is where the VLAN information is stored).
Incorrect Answers:
B, C: The configuration revision flag field, and the configuration revision reset switch don't exist in this context.

QUESTION 21:

If you needed to transport traffic coming from multiple VLANs (connected between switches), and your CTO was insistent on using an open standard, which protocol would you use?

A. 802.11B
B. spanning-tree
C. 802.1Q
D. ISL
E. VTP
F. Q.921

Answer: C

Explanation:
The act involved in the above question is trunking. The two trunking protocols in the answer choices are: 802.1Q and ISL. ISL is Cisco proprietary and IEEE 802.1Q is based on an open standard. When non-Cisco switches are used along with Cisco switches and trunking is required, it is best to use the 802.1Q encapsulation.
Incorrect Answers:
A: This standard is used in wireless networking and has nothing to do with VLAN switching.
B: The Spanning Tree Protocol (STP) is used to prevent loops within a bridged network.

Each VLAN runs a separate instance of the STP and this is enabled by default.
D: This is the alternative Cisco proprietary method of trunking.
E: VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis. It is not used to actually transport VLAN traffic.
F: This is an ISDN signalling standard and is not related with VLAN switching.

QUESTION 22:

What is the method used to filter traffic being bridged within a VLAN?

A. Ethernet maps
B. Router ACLs
C. VLAN maps
D. IP ACLs

Answer: C

QUESTION 23:

Which of the following technologies would an Internet Service Provider use to support overlapping customer VLAN ID's over transparent LAN services?

A. 802.1q tunneling
B. ATM
C. SDH
D. IP Over Optical Networking
E. ISL

Answer: A

Explanation:
Understanding How 802.1Q Tunneling Works:
The 802.1Q tunnelling feature supports secure virtual private networks (VPNs). 802.1Q tunnelling enables service providers to keep traffic from different customers segregated in the service provider infrastructure while significantly reducing the number of VLANs required to support the VPNs. 802.1Q tunnelling allows multiple customer VLANs to be carried by a single VLAN on the Catalyst 6000 family switch without losing their unique VLAN IDs.
When you configure 802.1Q tunnelling on the Catalyst 6000 family switch, traffic to be tunnelled comes into the switch from an 802.1Q trunk port on a neighboring device and enters the switch through a port configured to support 802.1Q tunnelling (a tunnel port). When the tunnel port receives traffic from an 802.1Q trunk port, it does not strip the 802.1Q tags from the frame header but, instead, leaves the 802.1Q tags intact and puts all the received 802.1Q traffic into the VLAN assigned to the tunnel port. The VLAN assigned to the tunnel port then carries the tunnelled customer traffic to the other

neighboring devices participating in the tunnel port VLAN. When the tunnelled traffic is received by an 802.1Q trunk port on a neighboring device, the 802.1Q tag is stripped and the traffic is removed from the tunnel.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_guide_chapter09186a008007f

---

QUESTION 24:

If you were to configure an ISL Ethernet trunk between two Cisco switches, named CK1 and CK2 , what would you have to include at the end of the link for the trunk to operate correctly? (Select two)

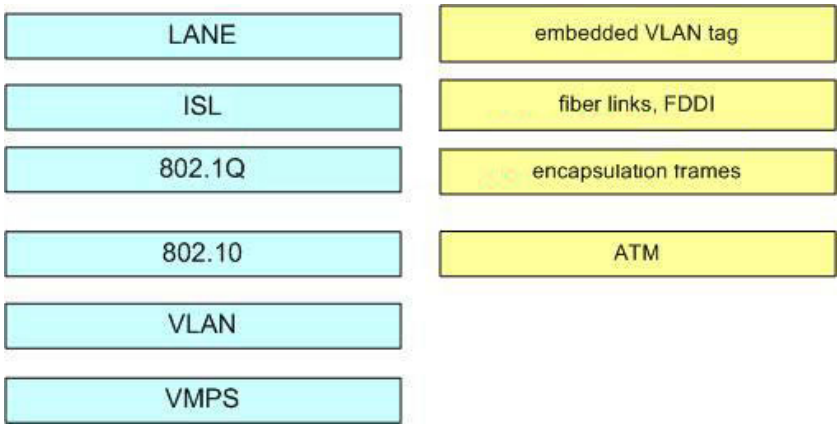
A. An identical VTP mode.
B. An identical speed/duplex.
C. An identical trunk negotiation parameter.
D. An identical trunk encapsulation parameter.

Answer: B, D

Explanation:
In order for a trunk to be operational, the speed and duplex settings must match at each end of the trunk, and both switches must use the same trunking encapsulation (802.1Q or ISL).
Incorrect Answers:
A: It is common for switches to have trunk links operating, while the VTP modes differ. For example, a switch configured with VTP mode server can have a trunk connected to a switch with VTP mode client.
C: This is incorrect, as there are a number of configurations that are supported where the trunk negotiation parameters differ between switches. For example, switch CK1 could have the trunk configured for "on" while switch CK2 could have the switch trunk configured for "desirable" and the trunk would be operational.

QUESTION 25:

DRAG DROP
Drag-and-drop the technology term on the left to the correct options column on the right (not all of the options will be used.)



Answer:

Explanation:
LANE - ATM
ISL - Encapsulation frames
802.1Q - embedded VLAN tag
802.10 - Fiber links, FDDI
VLAN
VMPS
1. LANE - LAN Emulation - An IEEE standard method for transporting VLANs over Asynchronous Transfer Mode (ATM) networks.
2. ISL - A Cisco Proprietary encapsulation protocol for interconnection multiple switches.
3. 802.1Q - An IEEE standard method for identifying VLANs by inserting a VLAN identifier into the frame header. This process is called frame tagging.
4. 802.10 - A Cisco Proprietary method of transporting VLAN information inside the standard 802.10 frame (Fiber Distributed Data Interface [FDDI]).
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 99

QUESTION 26:

You are the network administrator at Certkiller and switch CK1 is configured as shown below:
Interface gigethernet 0/1
Switchport mode trunk
Switchport trunk encapsulation dot1q
Switchport trunk native vlan 5
If untagged frames are arriving on interface gigethernet 0/1 of CK1 , which of the following statement are correct?

A. Untagged frames are automatically assumed to be in VLAN 5.
B. Untagged frames are defaulted to VLAN 1 traffic.
C. Untagged frames are dropped because all packets are tagged when dot1q trunked.
D. Untagged frames are determined on the other switch

E. Untagged frames are not supported on 802.1Q trunks.

Answer: A

Explanation:
Each physical port has a parameter called PVID. Every 802.1Q port is assigned a PVID value that is of its native VLAN ID (default is VLAN 1). All untagged frames are assigned to the LAN specified in the PVID parameter. When a tagged frame is received by a port, the tag is respected. If the frame is untagged, the value contained in the PVID is considered as a tag. All untagged frames will be assigned to the native VLAN. The native VLAN is 1 by default, but in this case the native VLAN is configured as VLAN 5 so choice A is correct.

QUESTION 27:

If you were to set up a VLAN trunk over a Fast Ethernet link on switch CK1 , which trunk mode would you set the local port to on CK1 if you wanted it to respond to requests from its link partner (CK2) and become a trunk?

A. Auto
B. Negotiate
C. Designate
D. Nonegotiate

Answer: A

Explanation:
Only ports in desirable and auto mode will negotiate a channel (either desirable-auto or desirable-desirable). Ports in on mode will only form a functional channel with other ports in on mode (they will not negotiate a channel with ports in desirable or auto mode).
Reference: Cisco, Troubleshooting Tips
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/trbl_ja.htm

---

QUESTION 28:

Which of the following trunking modes are unable to request their ports to convert their links into trunk links? (Select all that apply)

A. Negotiate
B. Designate
C. Nonegotiate
D. Auto
E. Manual
F. Off

Answer: C, D

Explanation:
Auto is a trunking mode but does not actively negotiate a trunk. It requires opposite side to be trunk or desirable, and will only respond to requests from the other trunk link. No-negotiate will configure the link to be unable to dynamically become a trunk; since no requests will be sent it will not respond to requests from other trunk links from a different switch.
Incorrect Answers:
A, B, E, F: These choices are wrong because they are not valid trunking modes

---

QUESTION 29:

ISL is being configured on a Certkiller switch. Which of the following choices are true regarding the ISL protocol? (Select two)

A. It can be used between Cisco and non-Cisco switch devices.
B. It calculates a new CRC field on top of the existing CRC field.
C. It adds 4 bytes of protocol-specific information to the original Ethernet frame.
D. It adds 30 bytes of protocol-specific information to the original Ethernet frame.

Answer: B, D

Explanation:
ISL adds a total of 30bytes to the Ethernet frame. A 26 byte header (10bytes identifies the VLAN ID) and a 4 byte trailer (containing a separate CRC).
Incorrect Answers:
A: This is incorrect because ISL is Cisco proprietary and can only be used on Cisco devices. For configuring a trunk to a non-Cisco switch, 802.1Q encapsulation should be used.
C: This is incorrect because it is contradictory to D. 30 byes are added with ISL, not 4 bytes. This choice describes what is used in 802.1Q frames, not ISL

QUESTION 30:

You are the network administrator tasked with designing a switching solution for the Certkiller network. Which of the following statements describing trunk links are INCORRECT? (Select all that apply)

A. The trunk link belongs to a specific VLAN.
B. Multiple trunk links are used to connect multiple devices.
C. A trunk link only supports native VLAN.
D. Trunk links use 802.10 to identify a VLAN.
E. The native VLAN of the trunk link is the VLAN that the trunk uses if that link fails for any reason.

Answer: A, B, C, D

Explanation:
A trunk is a point-to-point link that transmits and receives traffic between switches or between switches and routers. Trunks carry the traffic of multiple VLANs and can extend VLANs across an entire network. 100BaseT and Gigabit Ethernet trunks use Cisco ISL (the default protocol) or industry-standard IEEE 802.1Q to carry traffic for multiple VLANs over a single link. Frames received from users in the administratively-defined VLANs are identified or tagged for transmission to other devices. Based on rules you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmission to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is transmitted to the target end station.
Incorrect Answers:
E: This statement is true, as untagged frames are always used with the native VLAN. The native VLAN is VLAN 1 by default in Cisco switches.

QUESTION 31:

A Certkiller switch port is configured as a trunk using 802.1Q encapsulation. Which three statements regarding the IEEE 802.1Q standard are true? (Select three)

A. The packet is encapsulated with a 26 byte header and a 4 byte FCS.
B. The IEEE 802.1Q frame format adds a 4 byte field to an Ethernet frame.
C. The IEEE 802.1Q frame retains the original MAC destination address.
D. The IEEE 802.1Q frame uses multicast destination of 0x01-00-0c-00-00
E. The 802.1Q protocol uses point-to-point connectivity.
F. The 802.1Q protocol uses point-to-multipoint connectivity.

Answer: B, C, E

Explanation:
802.1Q frames add 4 bytes to the Ethernet frame. The original MAC address is left unaltered so the destination MAC is not changed. Trunks are always defined in a point to point configuration, with two switch ports used as the endpoints.
Incorrect Answers:
A: This describes the frame that is added to an ISL encapsulated frame, not an 802.1Q frame.
D: The destination MAC address is not altered when trunks are configured.
F: All trunks are always configured in a point to point fashion, there is no method available to support point to multipoint trunk configurations.

QUESTION 32:

Which DTP switchport mode parameter would you use to set a switch port to actively send and respond to DTP negotiation frames on switch CK1 ?

A. access
B. trunk
C. no negotiate
D. dynamic desirable
E. dynamic auto

Answer: D

Explanation:
There are five DTP switchport modes, and you should be familiar with all of them.
Access:This puts the interface (access port) into permanent nontrunking mode.
The interface will generate DTP frames, negotiating with the neighboring interface 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: The interface actively attempts 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. This is the default mode for all Ethernet interfaces. If the neighboring interface is set to the access or non-negotiate mode, the link will become a non-trunking link.
Dynamicauto: This command makes the interface willing to convert the link to a trunk link if the neighboring interface is set to trunk or desirable mode. Otherwise, the link will become a non-trunking link.
Switchport mode trunk: This command 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.
Switchport nonegotiate: Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link; otherwise the link will be a non-trunking link.

QUESTION 33:

A switch port on CK1 is being configured to support 802.1Q trunking. Which of the following are true about 802.1Q trunking? (Select one)

A. Both switches must be in the same VTP domain.
B. The encapsulation type of both ends of the trunk does not have to match.
C. The native VLAN on both ends of the trunk must be VLAN 1.
D. 802.1Q trunking can only be configured on a Layer 2 port.
E. In 802.1Q trunking, all VLAN packets are tagged on the trunk link, except the native VLAN.

Answer: E

Explanation:

E is correct because, "frames from the native VLAN of an 802.1Q trunk are not tagged with the VLAN number."
Incorrect Answers:
B: This is incorrect because the encapsulations types do have to match or it won't work properly. You can't use 802.1Q on one side and ISL on the other. C is incorrect because the native VLAN doesn't necessarily have to be VLAN 1.
C: By default, the native VLAN is VLAN 1 but this can be effectively changed to a different VLAN and the trunk will still be functional.
Reference: http://www.cisco.com/warp/public/473/27.html

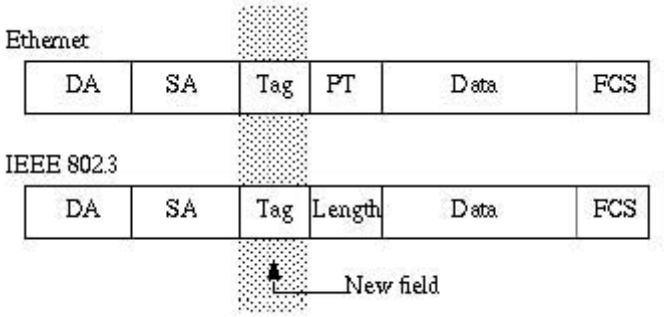
QUESTION 34:

A Certkiller switch is configured for 802.1Q trunking. What are valid characteristics of IEEE 802.1Q? (Select all that apply)

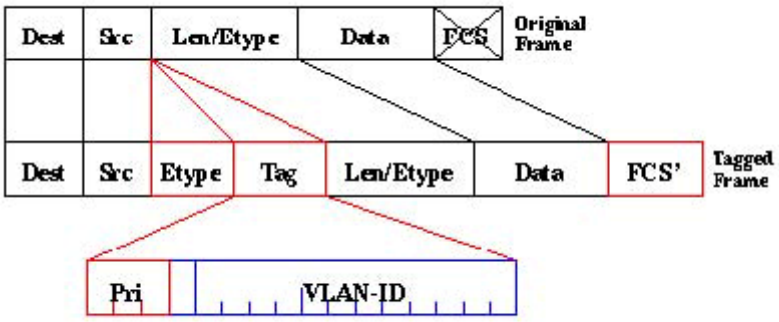
A. Use frame tagging.
B. None of the answers
C. It is a method for identifying VLANs
D. It inserts VLAN identifier into the frame header

Answer: A, C, D

Explanation:
802.1Q uses an internal tagging mechanism. Internal means that a tag is inserted within the frame (with ISL, the frame is encapsulated instead):



Note that on an 802.1Q trunk, one VLAN is NOT tagged. This VLAN, named the native VLAN, must be configured the same on each side of the trunk. This way, we can deduce to which VLAN a frame belongs when we receive a frame with no tag.
The tagging mechanism implies a modification of the frame; the trunking device inserts a 4-byte tag and recomputes the frame check sequence (FCS):



The EtherType field identifying the 802.1Q frame is 0x8100. In addition to the 12-bit VLAN-ID, 3 bits are reserved for 802.1p priority tagging.
Also, note that inserting a tag into a frame that already has the maximum Ethernet size creates a 1522 byte frame that can be considered as a "baby giant" by the receiving equipment. The 802.3 committee is extending the maximum standard frame size to address this issue.
.

QUESTION 35:

What are the reasons as to why an administrator would deploy Dynamic Trunking Protocol (DTP) on the Certkiller switched LAN? (Select all that apply)

A. For supporting auto-negotiation of IEEE 802.1Q trunks
B. For supporting auto-negotiation of ISL
C. For managing trunk negotiation in 2500 router supervisor engine software R 4.2 or later
D. For managing trunk negotiation in Catalyst supervisor engine software R 4.2 or later.
E. None of the above.

Answer: A, B, D

Explanation:
DTP was developed for the specific purpose of supporting automatic trunk negotiation for 802.1Q and ISL trunks. It is used only with Cisco Catalyst switches.
Incorrect Answers:
DTP is supported only on Cisco Catalyst switches. It is not supported on Cisco 2500 series routers.

QUESTION 36:

A fast Ethernet port on switch CK1 is configured as a trunk. What is true of this trunk link?

A. A trunk link only supports the native VLAN for a given port.

B. A trunk link uses 802.10 to identify VLANs over an Ethernet backbone.
C. A trunk link connects multiple devices on a single subnet to a switch port.
D. The native VLAN of the trunk link is the VLAN to which the port will belong if that link becomes non-trunk.
E. All of the above.

Answer: C

Explanation:
Trunks are used to connect multiple VLANs together. Individual switches configured with VLANs over the entire LAN subnet are connected to each other via a trunk port.
Incorrect Answers:
A: By default all VLANs within the range of 1 to 1000 is allowed to traverse the trunk port.
B: 802.10 is the standard used on FDDI networks and is not related to Ethernet VLAN trunks.
D: This is wrong because Native VLAN Number of the native VLAN for the trunk link (for 802.1Q trunks, the VLAN for which untagged traffic can be transmitted and received over the trunk; for ISL trunks, packets are tagged on all VLANs, including the native VLAN).

QUESTION 37:

You are a technician at Certkiller and your newly appointed trainee asks you what the Dynamic Trunking Protocol (DTP) mode 'desirable' means. What would your reply be?

A. The interface is put into permanent trunking mode but prevented from generating DTP frames.
B. The interface actively attempts to convert the link to a trunk link.
C. The interface is put into a passive mode, waiting to convert the link to a trunk link.
D. The interface is put into permanent trunking mode and negotiates to convert the link into a trunk link.

Answer: B

Explanation:
The DTP mode of desirable configured the trunk port to actively attempt to convert the link to a trunk link.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 105

QUESTION 38:

What would happen to a frame if a VLAN port configured as a trunk on the Catalyst switch CK1 were to receive an untagged frame?

A. The frame will cause an error message to be sent.
B. The frame will be dropped.
C. The frame will be processed as a native VLAN frame.
D. The frame will be tagged, and then processed as a native VLAN frame.

Answer: C

Explanation:
On an IEEE 802.1Q trunk port, all transmitted and received frames are tagged except for those on the VLAN configured as the native VLAN for the port. Frames on the native VLAN are always transmitted untagged and are normally received untagged. The default native VLAN is VLAN 1.
Reference:
http://www.cisco.com/en/US/products/hw/optical/ps2006/products_module_configuration_guide_chapter09186a

---

QUESTION 39:

Switch CK1 has a trunk link configured with IEEE 802.1Q encapsulation. What is the maximum Ethernet frame size on this trunk port?

A. 1496 Bytes
B. 1500 Bytes
C. 1518 Bytes
D. 1522 Bytes
E. 1548 Bytes

Answer: D

Explanation:
The 802.1q tag is 4 bytes; hence the resulting ethernet frame can be as large 1522 bytes (1518 for the maximum Ethernet frame size plus the 4 byte 802.1Q tag). The minimum size of the Ethernet frame with 802.1q tagging is 68 bytes.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK3 90/technologies_tech_note09186a0080094665.shtml

---

QUESTION 40:

The original frame is encapsulated and an additional header is added before the frame is carried over a trunk link. At the receive end, the header is removed and the frame is forwarded to the assigned VLAN. This describes which technology?

A. DISL
B. DTP
C. IEEE802.1Q
D. ISL

E. MPLS

Answer: D

QUESTION 41:

How does 802.1q trunking keep track of multiple VLANs?

A. modifies the port index of a data frame to indicate the VLAN
B. adds a new header containing the VLAN ID to the data frame
C. encapsulates the data frame with a new header and frame check sequence
D. tags the data frame with VLAN information and recalculates the CRC value

Answer: D

QUESTION 42:

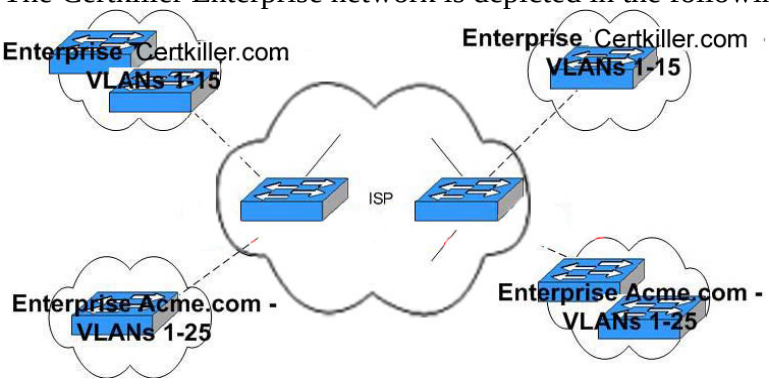
Which protocol inserts a four byte tag into the Ethernet frame and recalculates CRC value?

A. VTP
B. 802.1Q
C. DTP
D. ISL

Answer: B

QUESTION 43:

The Certkiller Enterprise network is depicted in the following topology exhibit:



An ISP is currently providing services to the enterprise Certkiller .com.
Certkiller .com is composed of a series of VLANs ranging from 1 to 15.
EnterpriseAcme.com is currently configured to support VLANs with the range of 1 to 25 and they're requesting support from the same ISP.
Which Layer 2 technology should the ISP use to keep the traffic segmented so Enterprise Certkiller .com and Enterprise Acme.com so that each can maintain their

current VLAN configurations?

A. Transparent LAN services
B. Metro Ethernet over DWDM
C. 802.1Q in Q
D. EoMPLS
E. L2TPv3

Answer: C

Explanation:
Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs. The IEEE 802.1Q-in-Q VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated.

QUESTION 44:

The Certkiller campus is utilizing the services of a Metro Ethernet provider. What is the function of VLAN tunnelling in this Metro Ethernet environment?

A. Renumbers their LANs.
B. Extends their logical network topology across wide geographic networks.
C. Provides combined wavelength routing.
D. Translates their VLANs at the service provider edge.

Answer: D

Explanation:
An ideal scenario to support multiple customers in the service provider environment would be to have customers utilizing any range of VLAN numbers while the service provider forwards the traffic independent of those VLAN IDs. By assigning a unique VLAN to each customer, the identity of multiple VLAN IDs from the customer site will not be lost. This builds a Layer 2 VPN where traffic from different business customers is segregated inside the service provider core and is dot1q tagged with appropriate VLAN IDs. Dot1q tunneling is in essence a 1q-in-1q technique that expands the VLAN space by retagging the tagged packets entering the service provider infrastructure. This is used to translate the customer's VLAN information at the provider edge, ensuring customer traffic separation will keeping the original VLAN information intact.
Reference:
http://www.cisco.com/en/US/netsol/ns110/ns221/ns223/ns227/networking_solutions_white_paper09186a00800a

---

QUESTION 45:

The Certkiller campus is utilizing the services of a Metro Ethernet provider, which is

using 802.1Q-in-Q. What's true about this Metro 802.1Q-in-Q model? (Select all that apply.)

A. Customer VLAN traffic is isolated from the service provide network's VLAN traffic.
B. Quality of service can be easily implemented using the Customer's ToS and CoS.
C. It has limited scalability in a service provider WAN.
D. Customer traffic retains original VLAN tags.
E. It provides efficient Layer 3 access.
F. It can connect disparate customer networks (Frame Relay, Ethernet, ATM, etc).

Answer: A, C, D

Explanation:
Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs. The IEEE 802.1Q-in-Q VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated. This is used to translate the customer's VLAN information at the provider edge, ensuring customer traffic separation will keeping the original VLAN information intact.
Incorrect Answers:
B: QoS services become difficult to manage and implement in metro Ethernet networks.
E: Layer 2 access is granted, since the customer handoff from the service provider is an Ethernet port.
F: This is used to connect Ethernet-only networks within a Metropolitan area Network, and other encapsulation types (ATM, Frame-Relay, PPP, HDLC, etc) are not supported.

QUESTION 46:

You are a network administrator at Certkiller and the CTO has asked you to allow a customer's LAN traffic to be transmitted on a single VLAN across multiple service provider networks. Which technology would you use?

A. Transparent LAN Services
B. Metro network segmentation
C. VLAN tunneling
D. OC 192
E. DWDM

Answer: C

Explanation:
Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks.
Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2

protocol configurations of each customer without impacting the traffic of other customers. VLAN tunneling is used to translate the customer's VLAN information at the provider edge, ensuring customer traffic separation will keeping the original VLAN information intact.
Reference:
http://www.cisco.com/en/US/products/hw/optical/ps2006/products_module_configuration_guide_chapter09186a

---

QUESTION 47:

What are the reasons for deploying VLANs? (Select all that apply)

A. to address the addition of network management through layer 3 routing protocols.
B. to address the redundancy issues of a flat network topology
C. to address the performance issues of a non-flat network topology
D. to address the scalability issues of a flat network topology

Answer: A, D

Explanation:
There are several benefits to using VLANs. In summary, VLAN architecture benefits include:
1. Increased performance
2. Improved manageability
3. Network tuning and simplification of software configurations
4. Physical topology independence
5. Increased security options
Increased performance
Switched networks by nature will increase performance over shared media devices in use today, primarily by reducing the size of collision domains. Grouping users into logical networks will also increase performance by limiting broadcast traffic to users performing similar functions or within individual workgroups. Additionally, less traffic will need to be routed, and the latency added by routers will be reduced.
Improved manageability
VLANs provide an easy, flexible, less costly way to modify logical groups in changing environments. VLANs make large networks more manageable by allowing centralized configuration of devices located in physically diverse locations.
Network tuning and simplification of software configurations
VLANs will allow LAN administrators to "fine tune" their networks by logically grouping users. Software configurations can be made uniform across machines with the consolidation of a department's resources into a single subnet.
Physical topology independence
VLANs provide independence from the physical topology of the network by allowing physically diverse workgroups to be logically connected within a single broadcast domain. If the physical infrastructure is already in place, it now becomes a simple matter to add ports in new locations to existing VLANs if a department expands or relocates.

VLANs have the ability to provide additional security not available in a shared media network environment. By nature, a switched network delivers frames only to the intended recipients, and broadcast frames only to other members of the VLAN. This allows the network administrator to segment users requiring access to sensitive information into separate VLANs from the rest of the general user community regardless of physical location. In addition, monitoring of a port with a traffic analyzer will only view the traffic associated with that particular port, making discreet monitoring of network traffic more difficult.

QUESTION 48:

The Certkiller network consists of numerous VLANs. Which two statements characterize VLANs? (Select two)

A. All hosts in the same VLAN are in the same broadcast domain.
B. All hosts in the same VLAN are in the same collision domain
C. VLAN membership is based upon port membership or assigned dynamically based on MAC.
D. It is a physical network segment.
E. They must be created in the vlan database mode on all IOS and Cat OS based Catalyst Switches.

Answer: A, C

Explanation:
At the most basic level, a VLAN is nothing more than a broadcast domain. The only difference between a traditional broadcast domain and one defined by a VLAN is that traditionally a broadcast domain has been seen as a distinct physical entity whose boundaries consist of a router. In fact, VLANs are very similar - their boundaries are also defined by a routing device, just like any broadcast domain. However, a VLAN is a logical construct, meaning that hosts are not necessarily groups within the physical confines of a traditional broadcast domain.
Switched networks by nature will increase performance over shared media devices in use today, primarily by reducing the size of collision domains. Grouping users into logical networks will also increase performance by limiting broadcast traffic to users performing similar functions or within individual workgroups. Additionally, less traffic will need to be routed, and the latency added by routers will be reduced.
A host can only become a member of any particular VLAN via one of two methods: static VLAN membership or dynamic VLAN membership. Static VLANs are configured at the port level, meaning that when a switch port is configured for a particular VLAN, any device plugged into that port becomes part of that VLAN. Dynamic VLAN membership is performed at the MAC level. No matter where a user is plugged in, the information pertaining to the MAC address of the station is used (normally via a VMPS server) to determine which VLAN the station belongs to.

QUESTION 49:

The Certkiller network is in need of a robust network management application.
What is Cisco's flagship web based device management tool?

A. CWOS
B. CiscoView
C. CWIS
D. VLANDirector
E. Traffic Director
F. NetSYS
G. Open View
H. All of the above

Answer: B

Explanation:
CiscoView is a member of the CiscoWorks2000 family, a Web based device management application providing dynamic status, monitoring, and configuration information for the broad range of Cisco internetworking products. CiscoView displays a physical view of a device chassis, with color-coding of modules and ports for at-a-glance status. Monitoring capabilities display performance and other statistics. Configuration capabilities allow comprehensive changes to devices, given requisite security privileges are granted.

QUESTION 50:

VTP is configured on switch CK1 . Which of the following features were added in VTP version 2 that were not previously supported in VTP version 1? (Select two)

A. Supports Token Ring VLANs.
B. Allows VLAN consistency checks.
C. Saves VLAN configuration memory.
D. Reduces the amount of configuration necessary.
E. Allows active redundant links when used with spanning tree.

Answer: A, B

Explanation:
VTP Version 2 includes the following improvements: Token Ring VLAN support, TLV support, transparent mode, and Consistency checks.
Incorrect Answers:
C, D: These were not improvements added to VTP Version 2.
E: STP detects and prevents loops by logically disabling the redundant path ports so there are no active redundant links.

QUESTION 51:

The Certkiller switches are configured to use VTP. What's true about the VLAN trunking protocol (VTP)? (Select two)

A. VTP messages will not be forwarded over nontrunk links.
B. VTP domain names need to be identical. However, case doesn't matter.
C. A VTP enabled device which receives multiple advertisements will ignore advertisements with higher configuration revision numbers.
D. A device in "transparent" VTP v.1 mode will not forward VTP messages.
E. VTP pruning allows switches to prune VLANs that do not have any active ports associated with them.

Answer: A, D

Explanation:
VTP messages are only transmitted across trunk links.
If the receiving switch is in transparent mode, the configuration is not changed. Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.
Incorrect Answers:
B: The VTP domain name is case sensitive and it must be identical with the domain name configured on the VTP server.
C: This is incorrect because if a VTP client receives an advertisement with a higher revision number, it won't ignore it. In fact, the advertisement with a higher revision level takes precedence when the switch is configured in client mode.
E: VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. It does not prune the individual VLANs.

QUESTION 52:

Switch CK1 and CK2 both belong to the Certkiller VTP domain. What's true about the switch operation in VTP domains? (Select all that apply)

A. A switch can only reside in one management domain
B. A switch is listening to VTP advertisements from their own domain only
C. A switch is listening to VTP advertisements from multi domains
D. A switch can reside in one or more domains
E. VTP is no longer supported on Catalyst switches

Answer: A, B

Explanation:
A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured to be in only one VTP domain, and each VLAN has a name that is unique within a management domain.
Typically, you use a VTP domain to ease administrative control of your network or to account for physical boundaries within your network. However, you can set up as many or as few VTP domains as are appropriate for your administrative needs. Consider that VTP is transmitted on all trunk connections, including ISL, IEEE 802.1Q, 802.10, and LANE.
Switches can only belong to one management domain with common VLAN requirements, and they only care about the neighbors in their own domains.
Reference: CCNP Switching Exam Certification Guide: David Hucaby & Tim Boyles, Cisco Press 2001, ISBN 1-58720 000-7 page 114

QUESTION 53:

VTP devices in a network track the VTP revision number. What is a VTP configuration revision number?

A. A number for identifying changes to the network switch.
B. A number for identifying changes to the network router.
C. A number for identifying changes to the network topology.
D. None of the above.

Answer: C

Explanation:
The configuration revision number is a 32-bit number that indicates the level of revision for a VTP packet. Each VTP device tracks the VTP configuration revision number assigned to it, and most of the VTP packets contain the VTP configuration revision number of the sender.
This information is used to determine whether the received information is more recent than the current version. Each time you make a VLAN change in a VTP device, the configuration revision is incremented by one. In order to reset the configuration revision of a switch, change the VTP domain name and then change it back to the original name.
Incorrect Answers:
A: Not all switch configuration changes will impact the VTP revision number. Only changes made to the VLAN configuration will cause an increment in the revision number.
B: VTP revision numbers are only used on network switches configured for VTP and are not used by Cisco routers.
Reference: Understanding and Configuring VLAN trunk protocol (VTP) Document ID: 10558http://www.cisco.com/warp/public/473/21.html

---

QUESTION 54:

Switch CK1 is configured to use the VLAN Trunking Protocol (VTP). What does CK1 advertise in its VTP domain?

A. The VLAN ID of all known VLANs, the management domain name, and the total number of trunk links on the switch.
B. The VLAN ID of all known VLANs, a 1-bit canonical format (CF1 Indicator), and the switch configuration revision number.
C. The management domain name, the switch configuration revision number, the known VLANs, and their specific parameters.
D. A 2-byte TPID with a fixed value of 0x8100 for the management domain number, the switch configuration revision number, the known VLANs, and their specific parameters.
E. None of the above.

Answer: C

Explanation:
"Each switch participating in VTP advertises VLAN information, revision numbers, and VLAN parameters on its trunk ports to notify other switches in the management domain. VTP advertisements are sent as multicast frames. The switch intercepts frames sent to the VTP multicast address and processes them with its supervisory processor VTP frames are forwarded out trunk links as a special case.
The following global configuration information is distributed in VTP advertisements:
1. VLAN IDs (ISL and 802.1Q)
2. Emulated LAN names (for ATM LANE)
3. 802.10 SAID values (FDDI)
4. VTP domain name
5. VTP configuration revision number
6. VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
7. Frame format
Reference: CCNP Switching Exam Certification Guide: page 115, David Hucaby & Tim Boyles, Cisco Press 2001, ISBN 1-58720 000-7
Incorrect Answers:
A: The total number of trunk links is not advertised.
B: A CFI is not advertised.
D: The TPID is not advertised. The value of 0x8100 is used to identify an 802.1Q trunking tag.

QUESTION 55:

VTP switches use advertisements to exchange information with each other. Which of the following advertisement types are associated with VTP? (Select all that apply)

A. Domain advertisements
B. Advertisement requests from clients
C. Subset advertisements

D. Summary advertisements

Answer: B, C, D

Explanation:
VTP advertisements include:
1. Summary Advertisements - These go out every 5 minutes or ever time the VLAN topology changes, and lists of information about the management domain (VTP version, domain name, configuration revision number, timestamp, MD5 encryption hash code, & number of subset advertisements incoming). When there is a configuration change, summary advertisements are complimented by or more subset advertisements.
1. Subset advertisements - These are sent out by VTP domain servers after a configuration change. They list the specifics of the change (VLAN creation / deletion / suspension / activation / name change / MTU change) and the VLAN parameters (VLAN status, VLAN type, MTU, VLAN name, VLAN number, SAID value).
1. Avertisement Requests from Clients- VTP clients request specific VLAN information that they're lacking (ie. Client switch is reset and loses its database, or VTP domain membership changes) so they can be responded by summary and subset advertisements.
Reference: CCNP Switching Exam Certification Guide: pages 116-117 David Hucaby & Tim Boyles, Cisco Press 2001, ISBN 1-58720 000-7

QUESTION 56:

Switch CK1 is part of the Certkiller VTP domain. What's true of VTP Pruning within this domain? (Select all that apply)

A. it does not prune traffic from VLANs that are pruning-ineligible
B. VLAN 1 is always pruning-eligible
C. it will prune traffic from VLANs that are pruning-ineligible
D. VLAN 2 is always pruning-ineligible
E. None of the above.

Answer: A

Explanation:
By definition, pruning-ineligible VLANs can not be pruned. You can make specific VLANs pruning ineligible with the clear vtp pruneeligible vlan_range command. By default, VLANs 2-1000 are pruning-eligible. Since the default VLAN for any switch port in a Catalyst switch is VLAN 1, it is not eligible for pruning.
Incorrect Answers:
B: VLAN 1 is always pruning-ineligible
C: The opposite is true.
D: By default, VLANs 2-1000 are eligible to be pruned.

QUESTION 57:

What action should you execute if you wanted to enable VTP pruning on your entire management domain?

A. Enable VTP pruning on any client switch in the management domain.
B. Enable VTP pruning on any switch in the management domain.
C. Enable VTP pruning on every switch in the management domain.
D. Enable VTP pruning on a VTP server in the management domain.
E. Disable VTP pruning on a VTP server in the management domain.

Answer: D

Explanation:
Enabling VTP pruning on a VTP server allows pruning for the entire management domain. Enabling this on the VTP server will mean that the VTP pruning configuration will be propagated to all VTP client switches within the domain. VTP pruning takes effect several seconds after you enable it. By default, VLANs 2 through 1000 are pruning-eligible.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 117

QUESTION 58:

Switch CK1 is configured with VTP. Which two VTP modes will make CK1 capable of creating and deleting VLANs on itself? (Select two)

A. Client
B. Server
C. Transparent
D. Pass-through
E. No-negotiate

Answer: B, C

Explanation:
VTP Modes
You can configure a switch to operate in any one of these VTP modes:
1. Server-In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.
2. Client-VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
3. Transparent-VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive out their trunk interfaces.

If you configure the switch as VTP transparent, you can create and modify VLANs but the changes affect only the individual switch.
Incorrect Answers:
A: Clients can not modify, add, or delete any VLAN information.
D, E: These options are not valid VTP modes.

QUESTION 59:

When the Catalyst switch CK1 is enabled to use VTP, which information does it advertise on its trunk ports? (Select two)

A. VTP mode
B. STP root status
C. Negotiation status
D. Management domain
E. Configuration revision number

Answer: D, E

Explanation:
The VTP protocol maintains VLAN configuration consistency throughout the network by distributing VLAN information to the network. VLAN information is sent to network devices in advertisements that contain the VTP management domain name, the current configuration revision number, the VLANs that the server knows about, and certain VLAN parameters. Any time you change a VLAN, VTP automatically sends an advertisement to update all other network devices.
The following global configuration information is distributed in VTP advertisements:
1. VLAN IDs (ISL and 802.1Q)
2. Emulated LAN names (for ATM LANE)
3. 802.10 SAID values (FDDI)
4. VTP domain name
5. VTP configuration revision number
6. VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
7. Frame format
Reference: Cisco, Configuring VTP
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_1/config/vtp.htm

---

QUESTION 60:

Is the following statement True or False?
MLS requires that MLS components be in the same VTP domain.

A. False
B. There is not enough information to determine
C. True

D. It could be true or false, depending on the type of switch.

Answer: C

Explanation:
MLS requires that MLS components, including the end stations, must be in the same Virtual Trunking Protocol (VTP) domain. VTP is a Layer 2 protocol used for managing VLANs on several Catalyst switches from a central switch. It allows an administrator to create or delete a VLAN on all switches in a domain without having to do so on every switch in that domain. The MultiLayer Switching Protocol (MLSP), which the MLS-SE and the MLS-RP use to communicate with one another, does not cross a VTP domain boundary.

QUESTION 61:

Which of the following VTP modes receives and forwards VTP updates, but does NOT participate in VTP synchronization?

A. Client
B. Server
C. Transparent
D. Pass-through

Answer: C

Explanation:
Transparent-VTP transparent network devices do not participate in VTP. A VTP transparent network device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent network devices do forward VTP advertisements that they receive out their trunking LAN ports.

QUESTION 62:

How can VTP pruning enhance network bandwidth?

A. By limiting the spreading of VLAN information.
B. By reducing unnecessary flooding of traffic to inactive VLANs.
C. By disabling periodic VTP updates.
D. By restricting unicast traffic to across VTP domains.
E. By updating unicast traffic periodically.

Answer: B

Explanation:
VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic,

such as broadcast, multicast, unknown, and flooded unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
Reference:
http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00800916

QUESTION 63:

Which of the following statements is NOT true regarding VTP?

A. Switches in VTP transparent mode will simply forward advertisements without processing them.
B. VTP reduces administrative overhead.
C. VTP pruning reduces overall network traffic.
D. VTP pruning is on by default.
E. All of the above are true statements.

Answer: D

Explanation:
By default, VTP pruning is disabled.
For VTP pruning to be effective, all devices in the management domain must either support VTP pruning or, on devices that do not support VTP pruning, you must manually configure the VLANs allowed on trunks.
Incorrect Answers:
A: This statement is true. Transparent VTP switches do not participate in the VTP process, but they do forward VTP information to other switches.
B, C: VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

QUESTION 64:

By what condition can a VTP version 2 switch operate in the same domain as a switch running VTP version 1?

A. VTP version 2 is disabled on the VTP version 2-capable switch
B. VTP version 2 is enabled on the VTP version 2-capable switch
C. VTP version 1 is disabled on the VTP version 2-capable switch
D. None of the above. VTP version 1 and version 2 are not compatible.

Answer: A

Explanation:

A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 provided VTP version 2 is disabled on the VTP version 2-capable switch (VTP version 2 is disabled by default). With VTP version 2 disabled, the switch will revert to version 1 to become backward compatible.

QUESTION 65:

Is the following statement True or False?
If you modified a VTP transparent switch, the changes you implement will affect all the switches in the network?

A. True
B. There is not enough information to determine
C. False

Answer: C

Explanation:
According to Cisco:
If you configure the switch as VTP transparent, you can create and modify VLANs but the changes affect only the individual switch. Transparent switches do not participate in VTP. Only changes made to a VTP switch in server mode will be propagated to all the other client switches within the network.

QUESTION 66:

Which of the following message types are associated with VTP header fields on a Cisco switched network? (Select all that apply)

A. Summary advertisements
B. Advertisement requests
C. VTP Join messages
D. Subset advertisement
E. None of the above.

Answer: A, B, C, D

Explanation:
The format of the VTP header can vary depending on the type of VTP message. However, they all contain the following fields in the header:
VTP protocol version: 1 or 2
VTP Message Types: Summary advertisements, Subset advertisement, Advertisement requests, VTP join messages, Management domain length, and Management domain name.

QUESTION 67:

In order for the Certkiller network to use VTP, which of the following conditions have to be met? (Select all that apply)

A. Trunking must be enabled between all Catalyst switches.
B. The Catalyst switches must be non-adjacent for trunking to be possible between them
C. The Catalyst switches must be adjacent.
D. Each Catalyst switch in a domain should be assigned the same VTP domain name.

Answer: A, C, D

Explanation:
According to the online documentation provided by Cisco:
In order to use VTP, you must assign a VTP domain name to each switch. VTP information will remain only within the same VLAN domain. The following are conditions for a VTP domain:
-Each Catalyst switch in a domain should be assigned the same VTP domain name.
-The Catalyst switches must be adjacent.
-Trunking must be enabled between all Catalyst switches.
If any one of the previous conditions is not met, the VTP domain is broken and information will not travel between the two separate parts.

QUESTION 68:

The Certkiller switches are all VTP enabled. What is true about VTP? (Select all that apply)

A. VTP version 2 is supported in supervisor engine software release 3.1(1) and later.
B. you must decide whether to use VTP version 1 or version 2.
C. VTP version 1 is supported in supervisor engine software release 2.1 or later
D. VTP version 1 is supported in ATM software release 3.1 or later.

Answer: A, B, C, D

Explanation:
According to Cisco Documentation:
If you use VTP in your network, you must decide whether to use VTP version 1 or version 2. VTP version 1 is supported in supervisor engine software release 2.1 or later and ATM software release 3.1 or later. VTP version 2 is supported in supervisor engine software release 3.1(1) and later.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007d

---

QUESTION 69:

In the Certkiller switched network VTP pruning has been enabled. What is the purpose of VTP pruning?

A. Enhancing network integrity
B. Enhancing network bandwidth use
C. Deploying AAA
D. Enhancing network security
E. Enhancing network load balancing

Answer: B

Explanation:
According to Cisco:
VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

QUESTION 70:

Switches CK1 and CK2 are both configured for transparent mode in the VTP domain. Which statement accurately describes these transparent VTP switches? (Select all that apply):

A. They do not synchronize VLAN configuration based on received advertisements
B. They do not participate in VTP
C. They do not advertise VLAN configuration
D. None of the above

Answer: A, B, C

Explanation:
VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive out their trunk ports.

QUESTION 71:

Is the following statement True or False?
When VTP v.2 is enabled on a switch, all of the version 2-capable switches in the domain power cycle (restart) automatically?

A. False

B. There is not enough information to determine
C. True

Answer: A

Explanation:
According to Cisco:
Although caution should be taken when enabling VTP version 2 on a switch, doing so will not cause all switches to power cycle. When you enable VTP version 2 on a switch, all of the version 2-capable switches in the domain enable VTP version 2. However, it will not cause all of the switches to reboot themselves.

QUESTION 72:

You are configuring switch CK1 for VTP. Which of the following are valid VTP operating modes that can be configured on CK1 ? (Select all that apply)

A. Server
B. Frontend
C. Client
D. Transparent
E. Backbone

Answer: A, C, D

Explanation:
There are only three VTP operating modes:
1) Server: These switches have full control in the creation and modification of VLANs. Servers advertise out all the VLAN information they receive, and they configure themselves in accord with whatever information they hear. Switches are in server mode by default.
2) Client: These switches listen to VTP advertisements, they modify their configuration as a result of what they hear, and they forward out VTP information to neighbouring switches; but they don't have the ability to: create, change, or delete VLANs.
3) Transparent: These switches don't participate in the VTP process. They don't advertise their VLAN configurations and they don't synchronize their database when they receive advertisements. In VTP version 1 a switch doesn't relay information it gets to the other switches but in VTP version 2 they do.

QUESTION 73:

The Certkiller switches are converting their VTP versions from 1 to version 2. Which of the following describe a benefit of using VTP v.2 over VTP v.1?

A. To save VLAN configuration memory
B. To reduce broadcast traffic carried on trunk lines.

C. To reduce the amount of configuration necessary.
D. To support token ring VLANs
E. None of the choices.

Answer: D

Explanation:
VTP version 2 supports the following features not supported in version1:
Token Ring support-VTP version2 supports Token Ring LAN switching and VLANs (Token Ring Bridge Relay Function [TrBRF] and Token Ring Concentrator Relay Function [TrCRF]).
Unrecognized Type-Length-Value (TLV) Support-A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM.
Version-Dependent Transparent Mode-In VTP version1, a VTP transparent network device inspects VTP messages for the domain name and version, and forwards a message only if the version and domain name match. Since only one domain is supported in the supervisor engine software, VTP version 2 forwards VTP messages in transparent mode, without checking the version.
Consistency Checks-In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP.

QUESTION 74:

Which of the following are true regarding the default values of a switch that is configured for VTP pruning? (Select two).

A. VLAN 1-1000 are pruning-eligible
B. VLAN 2-1000 are pruning-eligible
C. VLAN 1 is pruning-eligible
D. VLAN 1 is pruning-ineligible
E. VLAN 1-1023 is pruning-eligible
F. VLAN 1-1023 is pruning-ineligible

Answer: B, D

Explanation:
By default, VLANs 2-1000 are pruning-eligible. Since the default VLAN for any switch port in a Catalyst switch is VLAN 1, it is not eligible for pruning.

QUESTION 75:

Which of the following tasks are NOT functions performed by VTP switches? (Select all that apply)

A. To reduce parallel load sharing
B. To propagate global VLAN information
C. To provide routing randomness
D. To set the trunk priority levels of adjacent switches.
E. To ensure that there is a trunk operating in the network.

Answer: A, C, D, E

Explanation:
VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also called a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and that are interconnected with trunks. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.
The fundamental function of VTP is to manage, maintain, and propagate VLAN information throughout the enterprise network. All of the choices, besides B, describe functions that are not performed by VTP.

QUESTION 76:

The Certkiller network administrator is fine tuning the STP parameters on the Catalyst switches. In which states does the Spanning Tree protocol (STP) get affected by the forward delay parameter? (Select two)

A. Forwarding
B. Listening
C. Blocking
D. Disabled
E. Learning

Answer: B, E

Explanation:
The following states utilize information from the forward delay timer:
Listen - The switch listens for a period of time called the fwd delay (forward delay)
Learn - The switch learns for a period of time called the fwd delay (forward delay)
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 139

QUESTION 77:

Is the following statement True or False?
STP prevents redundant links.

A. False

B. True
C. There is not enough information to determine

Answer: A

Explanation:
According to Cisco:
STP runs on bridges and switches that are 802.1d-compliant. There are different flavors of STP, with IEEE 802.1d being the most popular and widely implemented. STP is implemented on bridges and switches in order to prevent loops in the network. STP should be used in situations where you want redundant links, but not loops.
Incorrect Answers:
B: STP prevents the use of redundant active links (by logically disabling the redundant ports) but redundant links are still supported, since the STP topology changes dynamically with the network. Redundant links can be used, but not more that one at a time since STP provides for no load balancing type of mechanism.

QUESTION 78:

If two paths to a root switch share the exact same path cost, what information will spanning tree use to determine the root port?

A. The lowest time to receive BPDUs.
B. The lowest Port ID.
C. The lowest sender bridge ID.
D. The highest MAC address on the receiving port.
E. None of the above.

Answer: C

Explanation:
A Root Bridge is chosen based on the results of the BPDU process between the switches. Initially, every switch considers itself the Root Bridge! When a switch first powers up on the network, it sends out a BPDU with its own BID as the Root BID. When the other switches receive the BPDU, they compare the BID to the one they already have stored as the Root BID. If the new Root BID has a lower value, they replace the saved one. But if the saved Root BID is lower, a BPDU is sent to the new switch with this BID as the Root BID. When the new switch receives the BPDU, it realizes that it is not the Root Bridge and replaces the Root BID in its table with the one it just received. The result is that the switch that has the lowest BID is elected by the other switches as the Root Bridge.
Based on the location of the Root Bridge, the other switches determine which of their ports has the lowest path cost to the Root Bridge. These ports are called Root Ports and each switch (other than the current Root Bridge) must have one.
The switches determine who will have Designated Ports. A Designated Port is the connection used to send and receive packets on a specific segment. By having only one Designated Port per segment, all looping issues are resolved!

Designated Ports are selected based on the lowest path cost to the Root Bridge for a segment. Since the Root Bridge will have a path cost of "0", any ports on it that are connected to segments will become Designated Ports. For the other switches, the path cost is compared for a given segment. If one port is determined to have a lower path cost, then it becomes the Designated Port for that segment. If two or more ports have the same path cost, then the switch with the lowest BID is chosen.

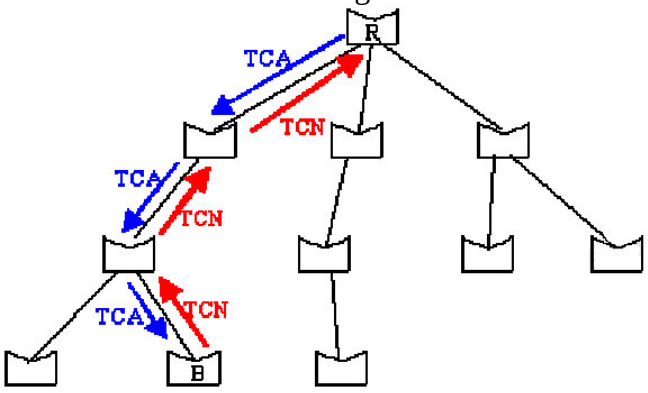
QUESTION 79:

What is true of a topology change in an STP environment?

A. The default aging time for MAC address entries will be reduced for a period of the max_age timer plus the forward_delay interval.
B. All ports will transition temporarily to the learning state for a period equal to the forward_delay interval.
C. All ports will temporarily transition to the learning state for a period equal to the max_age timer plus the forward_delay interval.
D. The default hello_timer for configuration BDPUs will be reduced for the period of the max_age timer.

Answer: C

Explanation:
In normal STP operation, a bridge keeps receiving configuration BPDUs from the root bridge on its root port. However, it never sends out a BPDU toward the root bridge. In order to achieve that, a special BPDU called the topology change notification (TCN) BPDU has been introduced. Therefore, when a bridge needs to signal a topology change, it starts to send TCNs on its root port. The designated bridge receives the TCN, acknowledges it, and generates another one for its own root port. The process continues until the TCN hits the root bridge.



Bridge B notifies a topology change by sending a TCN on its root port. The TCN is acknowledged and forwarded up to the root bridge R.

The TCN is a very simple BPDU that contains absolutely no information that a bridge sends out every hello_time seconds (this is locally configured hello_time, not the hello_time specified in configuration BPDUs). The designated bridge acknowledges the TCN by immediately sending back a normal configuration BPDU with the topology

change acknowledgement (TCA) bit set. The bridge that notifies the topology change does not stop sending its TCN until the designated bridge has acknowledged it. Therefore, the designated bridge answers the TCN even though it does not receive configuration BPDU from its root.
Broadcast the Event to the Network
Once the root is aware that there has been a topology change event in the network, it starts to send out its configuration BPDUs with the topology change (TC) bit set. These BPDUs are relayed by every bridge in the network with this bit set. As a result all bridges become aware of the topology change situation and it can reduce its aging time to forward_delay. Bridges receive topology change BPDUs on both forwarding and blocking ports.
The TC bit is set by the root for a period of max_age + forward_delay seconds, which is 20+15=35 seconds by default.
Reference:
Understanding Spanning-Tree Protocol Topology Changes
http://www.cisco.com/warp/public/473/17.html

QUESTION 80:

Multiple Certkiller switches are connected together, forming a loop in the network to provide redundancy. Which of the following technologies provides loop avoidance?

A. VTP
B. MLS-RP
C. MLS-SE
D. VTP Pruning
E. STP
F. STP Trunking
G. None of the above

Answer: E

Explanation:
Spanning-Tree Protocol (STP) is a Layer 2 protocol designed to run on bridges and switches. The specification for STP is defined in IEEE 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. STP detects/disables network loops and provides backup links between switches or bridges. It allows the device to interact with other STP compliant devices in your network to ensure that only one path exists between any two stations on the network.
Reference: http://www.zyxel.com/support/supportnote/ves1012/app/stp.htm

---

QUESTION 81:

Before a port can participate in the STP process the ports have to change. In which

sequence do the STP port states change through?

A. Initial, Learning, Updating, and Active
B. Blocking, Listening, Updating, and Active
C. Initial, Learning, Updating, and Forwarding
D. Blocking, Listening, Learning, and Forwarding

Answer: D

Explanation: The correct order is: blocking state (not participating), listening, learning (prepares to participate), and Forwarding.
Note: STP states:
1. Blocking-The Layer2 LAN port does not participate in frame forwarding
2. Listening-First transitional state after the blocking state when STP determines that the Layer2 LAN port should participate in frame forwarding
3. Learning-The Layer2 LAN port prepares to participate in frame forwarding
4. Forwarding-The Layer2 LAN port forwards frames
5. Disabled-The Layer2 LAN port does not participate in STP and is not forwarding frames.

QUESTION 82:

Is the following statement True or False?
The "show spanning-tree port-priority" command only displays information for ports with an active link?

A. False
B. There is not enough information to determine
C. True

Answer: C

Explanation:
According to Cisco:
The show spanning-tree port-priority command only displays information for ports with an active link. If these conditions are not met, enter a show running-config interface command to verify the configuration.

QUESTION 83:

Is the following statement True or False?
STP uses BPDU's (Bridge Data Units) to communicate and compute the spanning tree topology from each switch and in both directions from the route switch.

A. False
B. There is not enough information to determine

C. True

Answer: A

Explanation:
According to Cisco:
To communicate and compute the spanning tree topology, Bridge Protocol Data Units (BPDUs) are transmitted from each switch (configuration BPDUs) and in one direction from the root switch. Only one direction is used from the switch, not both.

QUESTION 84:

Which command would you enter to display a summary of the spanning-tree information? (Type in answer below)

Answer: show spantree summary

Explanation:
According to Cisco: Use the show spantree summary command to display a summary of spanning-tree information.

QUESTION 85:

In order for STP to run successfully on the Certkiller network, what standard the bridges and switches have to comply with?

A. 802.1c
B. 802.1e
C. 802.1x
D. 802.1f
E. 802.1d
F. 802.11

Answer: E

Explanation:
According to the online documentation provided by Cisco:
STP runs on bridges and switches that are 802.1d-compliant. There are different flavors of STP, with IEEE 802.1d being the most popular and widely implemented. STP is implemented on bridges and switches in order to prevent loops in the network. Use it in situations where you want redundant links, but not loops. Redundant links are important as backups in case of failover in a network. If your primary fails, the backup links are activated so that users can continue using the network. Without STP on the bridges and switches, such a situation could result in a loop.

QUESTION 86:

Switches CK1 and CK2 are exchanging Bridge Protocol Data Unit (BPDU) information. Which of the following can result from a BPDU exchange? (Select all that apply)

A. One switch is elected as the root switch.
B. Ports included in the spanning tree are selected.
C. The shortest distance to the root switch is calculated
D. A designated bridge for each LAN segment is selected.
E. A root port is selected.

Answer: A, B, C, D, E

Explanation:
A BPDU exchange between devices results in the following:
One switch is elected as the root switch.
The shortest distance to the root switch is calculated for each switch based on the path cost.
A designated bridge for each LAN segment is selected. This is the switch closest to the root bridge through which frames are forwarded to the root.
A root port is selected. This is the port providing the best path from the bridge to the root bridge.
Ports included in the spanning tree are selected.

QUESTION 87:

What determines the default spanning tree port path cost of STP devices within the Certkiller network?

A. The server speed settings
B. The available bandwidth.
C. The media speed of an interface.
D. The stored IOS settings
E. The interface number

Answer: C

Explanation:
The spanning tree port path cost default value is derived from the media speed of an interface. In the event of a loop, spanning tree considers port cost when selecting an interface to put into the forwarding state. You can assign lower cost values to interfaces that you want spanning tree to select first and higher cost values to interfaces that you want spanning tree to select last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks

other interfaces. The possible cost range is 1 through 200000000 (the default is media specific).

QUESTION 88:

Switch CK1 is a non-root switch in the Certkiller network. By what method does a non-Root switch choose its Root Port?

A. It chooses the port with the lowest cumulative Root Path Cost to the Root Bridge.
B. The port receives an inferior BPDU from a neighboring switch on a shard LAN segment.
C. It chooses the port with the highest cumulative Root Path Cost to the Root Bridge.
D. The port receives a BPDU announcing a higher Root Path Cost from a neighboring switch on a shared LAN segment.
E. None of the above.

Answer: A

Explanation:
The spanning tree Protocol uses the information found in the BPDUs to determine which ports should be forwarding and which should be blocking. If costs are equal, the STP reads through BPDU until it finds a parameter that is not equal. The lower port ID becomes the forwarding port, and the higher port ID is placed in a blocked state. As the BPDU prepares to leave a port, it applies a port cost. The sum of all the port costs is the path cost. Spanning Tree looks first at the path cost to decide which ports should forward and which should block. The port that reports the lowest path cost is chosen to forward.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 155

QUESTION 89:

What is the default transition time for a switch in the Certkiller switched LAN to move from blocking to forwarding state in the Spanning-Tree protocol?

A. 5 seconds
B. 50 seconds
C. 60 seconds
D. 90 seconds
E. 120 seconds

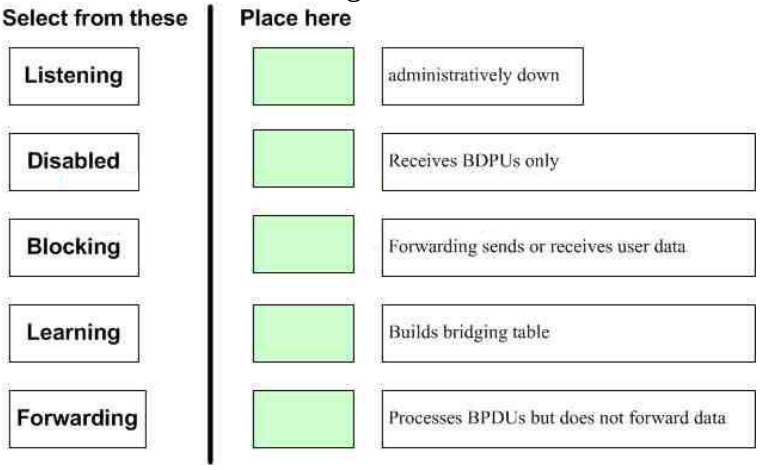
Answer: B

Explanation:
The default STP timers are shown below:
From blocking to listening 20 seconds
From listening to learning 15 seconds
From learning to forwarding 15 seconds

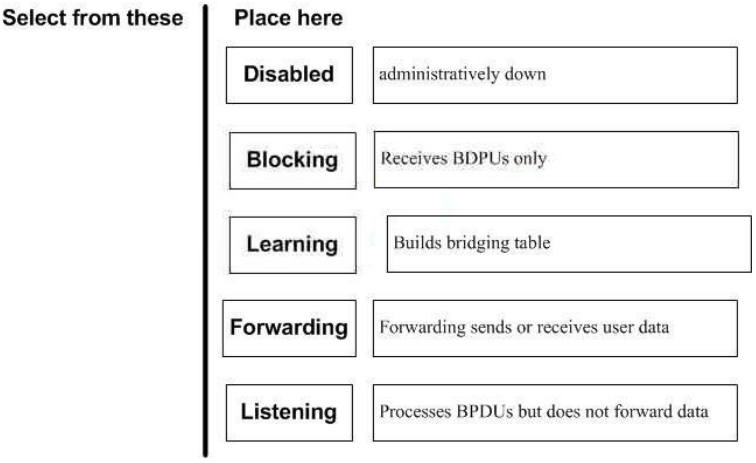
From blocking to forwarding state 50 seconds
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 141

QUESTION 90:

DRAG DROP
Drag the Spanning Tree Protocol state in the options column on the left to the matching
definition column on the right.



Answer:



Explanation:
Learning State:
A port in the learning state is preparing to participate in frame forwarding. This is the second transitional state through which a port moves in anticipation of frame forwarding. The port enters the learning state from the listening state through the operation of Spanning-Tree Protocol.
A port in the learning state performs the following functions:
Discards frames received from the attached segment.
Discards frames switched from another port for forwarding.

Incorporates station locations into its address database.
Receives BPDUs and directs them to the system module.
Receives, processes, and transmits BPDUs received from the system module.
Receives and responds to network management messages.

QUESTION 91:

Is the following statement True or False?
STP uses the port cost value when the interface is configured as an access port and it uses VLAN port cost values when the interface is configured as a trunk port.

A. There is not enough information to determine
B. False
C. True

Answer: C

Explanation:
According to Cisco:
Spanning tree uses the port cost value when the interface is configured as an access port and uses VLAN port cost values when the interface is configured as a trunk port.

QUESTION 92:

Switch CK1 is participating in the Spanning Tree Protocol (STP). What is true about STP Path Cost on a particular port of CK1 ?

A. It is known only to the local switch where the port resides.
B. It can be modified to help determine Root Bridge selection.
C. Modifying it can cause TCN BPDU to be sent to the Root Bridge.
D. When increased, it can provide higher bandwidth to a connecting port.
E. None of the above

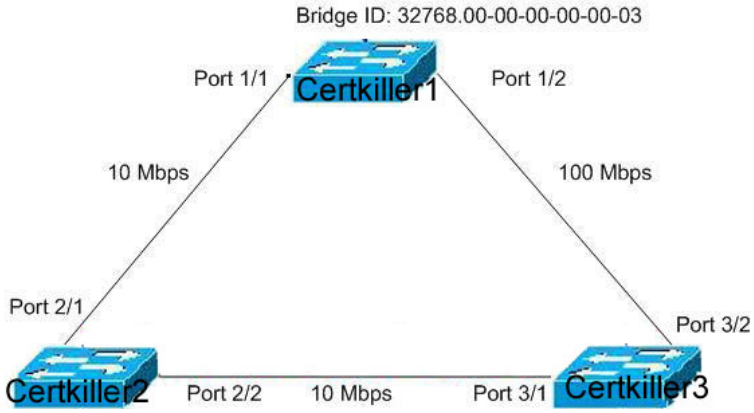
Answer: A

Explanation:
With STP, first a root bridge is elected. Then, the shortest distance to the root bridge is calculated for each switch based on the path cost. This calculation is done locally on each switch and the path cost for that switch is only used on the local switch.
Incorrect Answers:
B: Adjust the STP port priority, not the port path cost, can be done to influence the election of the root bridge.
C: A bridge considers it a topology change only when one of the following occurs:
1. When a port that was forwarding is going down (blocking for instance).
2. When a port transitions to forwarding and the bridge has a designated port. (This

means that the bridge is not standalone.)
TCN BPDUs are only sent to other switches within the network if one of the above happens.
D: Simply adjusting the cost value of the port will not make the port faster or provide for additional bandwidth throughput.

QUESTION 93:

Study the exhibit below:



Switch Certkiller 2 Switch Certkiller 3
Bridge ID: 32768.00-00-00-00-00-01 Bridge ID: 32768.00-00-00-00-00-02
Given the network configuration above and assuming that STP is enabled, which port will be elected the non-designated port?

A. Port 1/1
B. Port 1/2
C. Port 2/1
D. Port 2/2
E. Port 3/1
F. Port 3/2

Answer: B:

Explanation:
For each VLAN, the switch with the highest bridge priority (the lowest numerical priority value) is elected as the root bridge. If all switches are configured with the default priority value (32,768), the switch with the lowest MAC address in the VLAN becomes the root bridge.
The spanning tree root bridge is the logical center of the spanning tree topology in a switched network. All paths that are not required to reach the root bridge from anywhere in the switched network are placed in spanning tree blocking mode.
A spanning tree uses the information provided by BPDUs to elect the root bridge and root port for the switched network, as well as the root port and designated port for each switched segment.
In this example, since the priorities are set to the default, the switch with the lowest MAC

address is used as the tie breaker. In this case, Certkiller 2 will become the root switch, which means that port 3/1 and 1/1 will become the root ports and must be in the forwarding state. That leaves the other port on switch Certkiller 2, port 1/2 as the non-designated port since this switch has the highest MAC address.

QUESTION 94:

Which of the following specifications is a companion to the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) algorithm, and warrants the use multiple spanning-trees?

A. IEEE 802.1s (MST)
B. IEEE 802.1Q (CST)
C. Cisco PVST+
D. IEEE 802.1d (STP)

Answer: A

Explanation:
MST uses the modified RSTP version called the Multiple Spanning Tree Protocol (MSTP). MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than PVST+. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP]), and the Cisco PVST+ architecture.
MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This new architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).
In large networks, you can more easily administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanningtree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an MST region.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e

---

QUESTION 95:

Switch CK1 is powered on for the first time in the Certkiller network. Upon initial bootup, which destination address does a CK1 use to send BPDUs?

A. A well-known STP multicast address.
B. The IP address of its default gateway.
C. The MAC addresses stored in the CAM table.
D. The MAC address of neighbors discovered via CDP
E. None of the above

Answer: A

Explanation:
Bridge protocol data units (BPDUs) are used by the spanning tree algorithm to determine information about the topology of the network BPDUs are used to send configuration messages using multicast frames. When STP devices are first powered on, a well known multicast destination MAC address is used to send the BPDU information.
Incorrect Answers:
B: This would only send the BPDU information to the router. The other switches in the network that are participating in STP need the BPDU information, not the router.
C: When a switch is first powered up, the CAM table will be empty.
D: Since STP is standards based, it does not use any Cisco proprietary protocols such as CDP to perform any of its functions. This will ensure inter-operability with switches from other vendors.

QUESTION 96:

Switch CK3 is calculating the root path cost to the Root Bridge, CK1 . What is true regarding the Root Path cost?

A. It is the Path Cost of a particular Root Port.
B. It is the cost sent from the Root Bridge to all non-root bridges.
C. This value is the cumulative cost of all the links leading to the Root Bridge.
D. This value is the cumulative cost of all links sent from the Designated Port of the Root Bridge.

Answer: C

Explanation:
The first stage in the STP process is the calculation stage. During this stage, each bridge on the network transmits BPDUs that allow the system to work out:
1. The identity of the bridge that is to be the RootBridge- the central reference point from which the network is configured.
2. The Root Path Costs for each bridge - that is, the cost of the paths from each bridge to the Root Bridge. This value is found by adding up the cost of all of the links to the root bridge.
3. The identity of the port on each bridge that is to be the Root Port - the one that is connected to the Root Bridge using the most efficient path, that is, the one that has the lowest Root Path Cost. Note that the Root Bridge does not have a Root Port.

4. The identity of the bridge that is to be the Designated Bridge of each LAN segment - the one that has the lowest Root Path Cost from that segment. Note that if several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge.

QUESTION 97:

At which layer of the OSI model does the Spanning Tree Protocol (STP) operate at?

A. Layer 5
B. Layer 4
C. Layer 3
D. Layer 2
E. Layer 1

Answer: D

Explanation:
Spanning-Tree Protocol (STP) is a Layer 2 (L2) protocol designed to run on bridges and switches. The specification for STP is called 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. Loops are deadly to a network.

QUESTION 98:

Which of the following specification will allow you to: associate VLAN groups to STP instances so you can provide multiple forwarding paths for data traffic and enable load balancing?

A. IEEE 802.1d (STP)
B. IEEE 802.1s (MST)
C. IEEE 802.1Q (CST)
D. IEEE 802.1w (RSTP)

Answer: B

Explanation:
IEEE 802.1s MST Overview
MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than PVST+. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP]), and the Cisco PVST+ architecture.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e

QUESTION 99:

Is the following statement True or False?
STP prevents loop by forcing certain redundant data paths into a standby (blocked) state, while leaving others in a forwarding state.

A. False
B. True
C. There is not enough information to determine

Answer: B

Explanation:
According to Cisco:
STP forces certain redundant data paths into a standby (blocked) state, while leaving others in a forwarding state. If a link in forwarding state becomes unavailable, STP reconfigures the network and reroutes data paths by activating the appropriate standby path.

QUESTION 100:

You want to influence the root switch election process within the Certkiller network. When setting up STP in this network, which switch should you configure as the root switch?

A. The most centralized switch
B. The most secure switch
C. The most updated switch
D. The most powerful switch
E. The switch that has the longest uptime.

Answer: A

Explanation:
Cisco recommends using the most centralized switch in the network as the root switch.
According to Cisco:
Before configuring STP, you need to select a switch to be the root of the spanning tree. It does not necessarily have to be most powerful switch; it should be the most centralized switch on the network. All dataflow across the network will be from the perspective of this switch. It is also important that this switch be the least disturbed switch in the network. The backbone switches are often selected for this function, because they typically do not have end stations connected to them. They are also less likely to be disturbed during moves and changes within the network.

QUESTION 101:

You want to influence the Root Bridge election process in the Certkiller network. To do this, you are adjusting the Bridge ID values. What is Cisco's philosophy on the STP root selection process regarding the Root ID value?

A. Smaller is better (more preferred).
B. Larger is better (more preferred).
C. The bridge ID should always be zero

Answer: A

Explanation:
In the STP root selection process, a smaller value is preferred over a larger value. If the Root ID on Switch A is advertising an ID that is smaller than the Root ID that its neighbor (Switch B) is advertising, Switch A's information is better. Switch B stops advertising it's Root ID, and instead accepts that of Switch A.

QUESTION 102:

After you decide which switch should be the root switch, which command would you enter to give it priority in the selection process? (Type in answer below)

Answer: bridge priority

Explanation:
According to Cisco:
After you decide which switch should be the root switch, set the appropriate variables to designate it as the root switch. The only variable you have to set is the bridge priority. If this switch has a bridge priority that is lower than all other switches, it will be automatically selected by the other switches as the root switch.

QUESTION 103:

Which of the following factors are NOT used to determine the stable active spanning tree topology of the switched Certkiller network?

A. The port identifier associated with each Layer 2 interface
B. The port identifier associated with each Layer 3 interface
C. The spanning tree path cost to the root bridge
D. The unique bridge ID
E. All of the above are used.

Answer: B

Explanation:

The Spanning Tree Protocol does not use layer 3 information to determine the overall topology. Layer 3 interfaces do not participate in STP, since spanning tree is a layer 2 technology.
Incorrect Answers:
A, C, D: The stable active spanning tree topology of a switched network is determined by the following:
-The unique bridge ID (bridge priority and MAC address) associated with each VLAN on each switch
-The spanning tree path cost to the root bridge
-The port identifier (port priority and MAC address) associated with each Layer 2 interface

---

QUESTION 104:

The Spanning Tree Protocol is running on numerous Certkiller devices. Which of the following equipment types does STP run on in the Certkiller network? (Select all that apply):

A. switches
B. servers
C. routers
D. bridges
E. None of the above.

Answer: A, D

Explanation:
The Spanning-Tree Protocol (STP) is a Layer 2 (L2) protocol designed to run on bridges and switches. The specification for STP is called 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. Loops are deadly to a network.
Incorrect Answers:
B: Servers generally operate at layers 4-5, since they are used to run applications or to store data. They do not participate in STP.
C: Routers operate at layer 3 and do not participate in STP, since the STP function is used to detect and prevent bridging loops, not routing loops.

QUESTION 105:

A failure has occurred in the Certkiller switched network, causing a loop. What causes bridging loops to occur in a LAN?

A. A failure in the route-switch module
B. A failure in the VLAN tunnel
C. A failure in the VTP trunk
D. A failure in the STA

Answer: D

Explanation:
The primary function of the spanning-tree algorithm (STA) is to cut loops created by redundant links in bridged networks. The Spanning-Tree Protocol (STP) operates at Layer 2 of the OSI model and, by the means of bridge protocol data units (BPDUs) exchanged between bridges, elects the ports that will eventually forward or block traffic. This protocol can fail in some specific cases and troubleshooting the resulting situation can be very difficult, depending on the design of the network. We can even say that in this particular area, the most important part of the troubleshooting is done before the problem occurs. A failure in the STA generally leads to a bridging loop (not a spanning tree loop as you don't need STP to have a loop). Most customers calling the TAC for spanning tree problems are suspecting a bug, but experience proves that it is seldom the case. Even if the software is at stake, a bridging loop in a STP environment necessarily comes from a port that should block, but that is forwarding traffic.

QUESTION 106:

The bridge priority of switch CK1 is being manually configured. In the STP root selection process, what happens to the switch with the lowest priority in the network?

A. It is withdrawn from the election process.
B. It loses the root bridge election process.
C. It wins the root bridge election process.
D. None of the above. The bridge priority is not used to determine the root bridge.

Answer: C

Explanation:
As the BPDU goes out through the network, each switch compares the BPDU it sent out to the one it received from its neighbors. From this comparison, the switches come to an agreement as to who the root switch is. The switch with the lowest priority in the network wins this election process.

QUESTION 107:

If a layer 2 interface on switch CK1 uses the Spanning Tree Protocol (STP) which of the following states could it NOT possibly be in at any time?

A. Forwarding
B. Learning
C. Disabled
D. Blocking
E. Listening

F. None of the above

Answer: F

Explanation:
According to Cisco:
Each Layer 2 interface on a switch using spanning tree exists in one of the following five states:
Blocking-The Layer 2 interface does not participate in frame forwarding
Listening-First transitional state after the blocking state when spanning tree determines that the Layer 2 interface should participate in frame forwarding
Learning-The Layer 2 interface prepares to participate in frame forwarding
Forwarding-The Layer 2 interface forwards frames
Disabled-The Layer 2 interface does not participate in spanning tree and is not forwarding frames.

QUESTION 108:

Is the following statement True or False?
Cisco recommends manually configuring the hello time, forward delay time, and maximum age time after configuring the switch as the root bridge for optimal performance.

A. True
B. There is not enough information to determine
C. False

Answer: C

Explanation:
According to Cisco:
We recommend that you avoid manually configuring the hello time, forward delay time, and maximum age time after configuring the switch as the root bridge.

QUESTION 109:

When a network engineer designs a switch topology, they assign higher priority values to interfaces that they want spanning tree to select first and lower priority values to interfaces that they want spanning tree to select last. However, if multiple interfaces have equal priority values, spanning tree puts the interface with the _____ interface number in the forwarding state.

A. Neutral
B. Highest
C. Lowest
D. Random

E. First

Answer: C

Explanation:
In the event of a loop, spanning tree considers port priority when selecting an interface to put into the forwarding state. You can assign higher priority values to interfaces that you want spanning tree to select first and lower priority values to interfaces that you want spanning tree to select last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

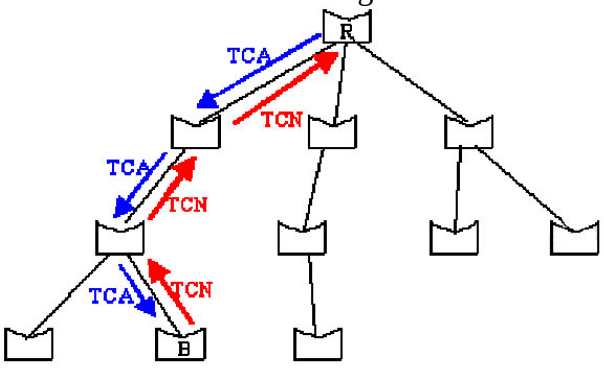
QUESTION 110:

When STP operation is functioning normally and after the topology has converged, which statement is true about BPDUs?

A. A bridge sends configuration BPDUs towards the root bridge every two seconds.
B. A bridge sends configuration BPDUs towards the root bridge every 15 seconds.
C. A bridge sends a TCN BPDU to the root bridge once upon initial configuration, followed by configuration BPDUs every two seconds.
D. A bridge sends only TCN BPDUs to the root bridge and no configuration BPDUs.

Answer: D

Explanation:
In normal STP operation, a bridge keeps receiving configuration BPDUs from the root bridge on its root port. However, it never sends out a BPDU toward the root bridge. In order to achieve that, a special BPDU called the topology change notification (TCN) BPDU has been introduced. Therefore, when a bridge needs to signal a topology change, it starts to send TCNs on its root port. The designated bridge receives the TCN, acknowledges it, and generates another one for its own root port. The process continues until the TCN hits the root bridge.



Bridge B notifies a topology change by sending a TCN on its root port. The TCN is acknowledged and forwarded up to the root bridge R.

The TCN is a very simple BPDU that contains absolutely no information that a bridge

sends out every hello_time seconds (this is locally configured hello_time, not the hello_time specified in configuration BPDUs). The designated bridge acknowledges the TCN by immediately sending back a normal configuration BPDU with the topology change acknowledgement (TCA) bit set. The bridge that notifies the topology change does not stop sending its TCN until the designated bridge has acknowledged it. Therefore, the designated bridge answers the TCN even though it does not receive configuration BPDU from its root.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK6 21/technologies_tech_note09186a0080094797.shtml

---

QUESTION 111:

After how long does it take for the port to change from blocking to forwarding when spanning-tree PortFast is enabled?

A. immediately
B. 15 seconds
C. 20 seconds
D. 30 seconds
E. 50 seconds

Answer: A

QUESTION 112:

Which two statements concerning STP state changes are true? Select two

A. Upon bootup, a port tran stions from blocking to forwarding because it assumes itself as root.
B. Upon bootup, a port tran stions from blocking to listening because it assumes itself as root.
C. Upon bootup, a port tran stions from listening to forwarding because it assumes itself as root.
D. If a forwarding port receives no BPDUs by the max_age time limit, it will transition to listening.
E. If a forwarding port receives an inferior BPDU, it will transition to listening.
F. If a blocked port receives no BPDUs by the max_age time limit, it will transition to listening.

Answer: B, F

QUESTION 113:

Which three statements about STP timers are true? Select three.

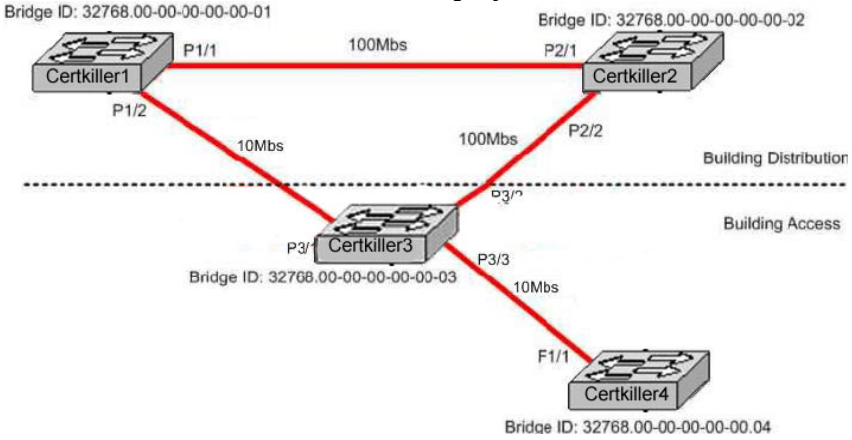
A. STP timers values (hello, forward delay, max age) are included in each BPDU

B. A switch is not concerned about its local configuration of the STP timers values. It will only consider the value of the STP timers contained in the BPDU it is receiving.
C. To successfully exchange BPDUs between two switches, their STP timers value (hello, forward delay, max age) must be the same.
D. If any STP timer value (hello, forward delay, max age) needs to be changed, it should at least be changed on the root bridge and backup root bridge.
E. On a switched network with a small network diameter, the STP hello timer can be tuned to a lower value to decrease the load on the switch CPU.
F. The root bridge passes the timer information on BPDUs to all routers in the Layer 3 configuration.

Answer: A, B, D

QUESTION 114:

The Certkiller switched LAN is displayed below:



Your junior network administrator has just finished installing the above switched network using Cisco 3550s and would like to manipulate the root bridge election. Which switch should he configure as the root bridge and with which command?

A. Certkiller 1(config)# spanning-tree vlan 1 priority 4096
B. Certkiller 2(config)# set spanning-tree priority 4096
C. Certkiller 3(config)# spanning-tree vlan 1 priority 4096
D. Certkiller 1(config)# set spanning-tree priority 4096
E. Certkiller 2(config)# spanning-tree vlan 1 priority 4096
F. Certkiller 3(config)# set spanning-tree priority 4096

Answer: E

QUESTION 115:

What is the default priority value assigned to a switch when STP is enabled?

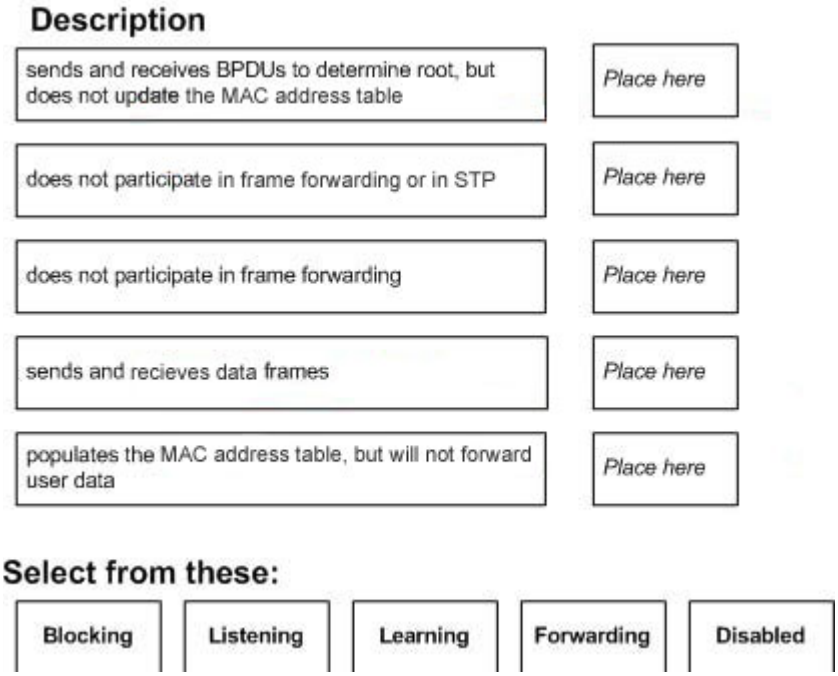
A. 1
B. 255

C. 4096
D. 32,768
E. 65,536

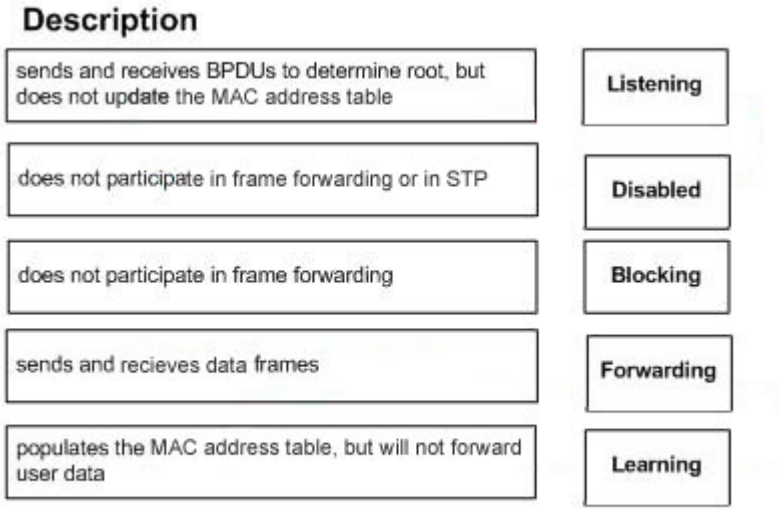
Answer: D

QUESTION 116:

DRAG DROP
As a Certkiller .com administrator you are required to drag the port states to their correct description.



Answer:



Select from these:

QUESTION 117:

You are in the midst of configuring a Cisco 5000 Catalyst switch named CK1 and you want to control the amount of broadcasts on the network. To control these broadcasts, you create some VLANs on CK1 . Which hardware would you use to configure inter-VLAN communication in this scenario?

A. MLS
B. RSM
C. MSFC
D. VLAN bandwidth

Answer: B

Explanation:
You can view a Route Switch Module (RSM) as an external router that has several interfaces directly connected into the different VLANs of a Catalyst 5000 switch. The RSM is the internal routing processor that lies within the Catalyst 5000 switch. To provide for inter-vlan communication, traffic must pass through the RSM or an external router.
Reference: Troubleshooting InterVLAN Routing on a Catalyst 5000 Switch with RSM
http://www.cisco.com/warp/public/473/56.html
Incorrect Answers:
A: MLS is Multilayer Switching (MLS) and is not used in the Catalyst 5000.
C: The Multilayer Switch Feature Card (MSFC) is a Route Processor (RP).
D: This choice does not apply

QUESTION 118:

The Certkiller switch CK1 must recognize the router as _____ for MLS to function in the network.

A. A netflow card
B. An MLS-RP
C. An MLS-SE
D. An MLS-RE

Answer: B

Explanation:
For MLS to function, the switch must recognize the router as an MLS-RP. Internal MLS-RPs (the RSM or RSFC in a Catalyst 5000 family member and the MSFC in a Catalyst 6000 family member) are automatically recognized by the MLS-SE in which they are installed. For external MLS-RPs, one must explicitly inform the switch of the router's address. This address is not actually an IP address, although on external MLS-RPs it is chosen from the list of IP addresses configured on the router's interfaces. It is simply a router ID. For internal MLS-RPs, the MLS-ID is normally not even an IP address configured on the router. Since internal MLS-RPs are included automatically, it is commonly a loopback address (127.0.0.x). For MLS to function, include on the MLS-SE the MLS-ID found on the MLS-RP.

QUESTION 119:

You need to quickly confirm the status of an interface in the Certkiller switch. What show command could you use to confirm whether or not an MLS-RP interface is an 'up/up' state on a router?

A. show ip interface brief
B. show ip brief
C. show interface brief ip
D. show interface brief

Answer: A

Explanation:
The correct command is (show ip interface brief). All the other choices are incorrect commands. The command (show ip interface) is a valid command, but it gives you much more detail. Since you are only interested on confirming the up/up states, the (show ip interface brief) command is ideal.

QUESTION 120:

Is the following statement True or False regarding a Catalyst 6000 switch named

CK1 ?
The Catalyst 6000 family of switches supports the use of an external MLS-RP?

A. There is not enough information to determine
B. True
C. False

Answer: C

Explanation:
According to Cisco:
The Catalyst 6000 family of switches does not support an external MLS-RP at this time.
The MLS-RP must be an MSFC.

QUESTION 121:

The Certkiller network is adding devices that are capable of MLS. A Cisco Catalyst 5000/5500 switch with a NetFlow Feature card can perform MLS with which three devices? (Select three.)

A. RSM
B. RSFC
C. Catalyst 8500
D. Catalyst 2948G-L3
E. Catalyst 2900

Answer: A, B, C

Explanation:
A: Cisco IOS running on the RSM has the ability to instruct the NFFC hardware.
B: The RSFC (Route Switch Feature Card) or Route Switch Module (RSM) performs the route processing on the Catalyst switch with a NFFC-II
C: Routing Processing services can also be provided by an externally attached Catalyst 6000 with an MSM (currently supports unicast MLS only), Catalyst 8500, Cisco 7500, 7200, 4700, 4500, 3640 or 3620.
Note: The NetFlow Feature Card increases IP Multilayer Switching (MLS) performance.
Reference: Product Bulletin, No. 909, Catalyst 4000 and 5000 Family Supervisor Engine Software

---

QUESTION 122:

Is the following statement True or False?
The MLS-RP can be internal but can not be external?

A. True
B. False

C. There is not enough information to determine

Answer: B

Explanation:
The MLS-RP can be internal (installed in a switch chassis) or external (connected via a cable to a trunk port on the switch). Examples of internal MLS-RPs are the Route Switch Module (RSM) and the Route Switch Feature Card (RSFC), which are installed in a slot or supervisor of a Catalyst 5000 family member, respectively.

QUESTION 123:

You are the administrator of the Certkiller network and you are configuring one of the switches. While doing so, you add the following configuration command to switch CK1 :
"mls rp ip"
What is the purpose of this command?

A. For enabling MLSP
B. For placing an external route processor in the interface of the VTP domain switch
C. For assigning VLAN ID to route processor interface
D. For enabling the RSM interface
E. For entering into the router interface

Answer: A

Explanation:
Multi-Layer Switching (MLS) has become a highly desired method of accelerating routing performance through the use of dedicated Application Specific Integrated Circuits (ASICs). Traditional routing is done through a central CPU and software. MLS offloads a significant portion of routing (packet rewrite) to hardware, and thus has also been termed switching. MLS and Layer 3 switching are equivalent terms.
To enable the Multilayer Switching Protocol (MLSP), use the mls rp ip global configuration command. MLSP is the protocol that runs between the switches and routers. Use the no form of this command to disable MLS.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/switch_r/xrmls.htm#1017390

QUESTION 124:

While logged into a Certkiller multilayer switch, you type in the following command:
interface
What is this command for?

A. for enabling the RSM interface
B. for entering into the router interface

C. for placing an external route processor in the interface of the VTP domain switch
D. for assigning VLAN ID to route processor interface
E. for enabling MLSP

Answer: B

Explanation:
This is a trick question with a very simple answer. If you want to configure the actually MLS Route Processor you have to get out of global mode and into interface mode
Switch(config-if)#

QUESTION 125:

You are the administrator of the Certkiller network and you are configuring one of the switches. While doing so, you add the following configuration command to switch CK1 :
"Mls rp vlan-id"
What is this command used for?

A. for enabling MLSP
B. for assigning VLAN ID to route processor interface
C. for enabling the RSM interface
D. for placing an external route processor in the interface of the VTP domain switch
E. for entering into the router interface

Answer: B

Explanation:
Use this command to assign a VLAN ID to an interface. RSM VLAN interfaces or ISL-encapsulated interfaces do not require the VLAN ID to be assigned.
To assign a VLAN ID, use the mls ip vlan-id interface configuration command.
The following example assigns a VLAN ID of 23 to the current interface:
"mls rp vlan-id 23"
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/switch_r/xrmls.htm#1017566

QUESTION 126:

Which hardware component do standard and extended access lists use to deny traffic at wire speed?

A. NetFlow Feature Card
B. Catalyst Switch Supervisor Engine III
C. Multilayer Switch Feature Card
D. MultiLayer Switching Route Processor
E. None of the above.

Answer: D

Explanation:
MLS allows you to enforce access lists on every packet of the flow without compromising MLS performance. When you enable MLS, the MLS-SE handles standard and extended access list permit traffic at wire speed.
NoteAccess list deny traffic is always handled by the MLS-RP, not the MLS-SE.
Route topology changes and the addition or modification of access lists are reflected in the MLS switching path automatically on the MLS-SE. The techniques for handling route and access list changes apply to both the RSM and directly attached external routers.
For example, when Station A wants to communicate with Station B, it sends the first packet to the MLS-RP. If an access list is configured on the MLS-RP to deny access from Station A to StationB, the MLS-RP receives the packet, checks the access list to see if the packet flow is permitted, and discards the packet based on the access list. Because the first packet for this flow does not return from the MLS-RP, an MLS cache entry is not established by the MLS-SE
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps679/products_configuration_guide_chapter09186a008007e

---

QUESTION 127:

MLS is running on the Certkiller network. Which MLS component do the MLS-RP and the MLS-SE use to communicate with one another? (Type in answer below)

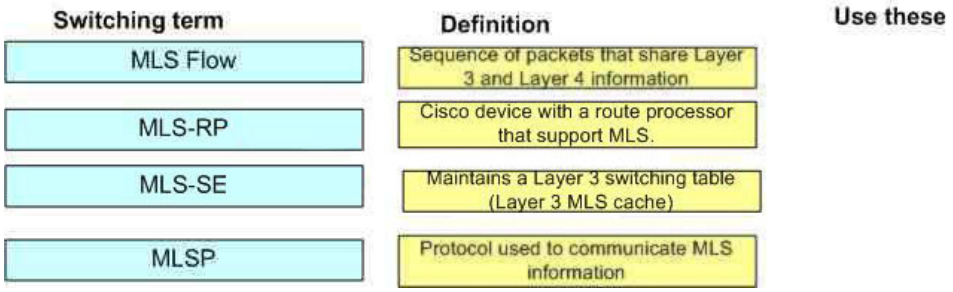
Answer: MLSP

Explanation:
MLSP is the protocol that runs between the MLS-SE and the MLS-RP. MLSP is utilized by the MLS-RP and the MLS-SE to communicate with one another; tasks include enabling MLS; installing, updating or deleting
flows (cache information); and managing
and exporting flow statistics (Netflow Data Export is covered in other documentation).
MLSP also allows the MLS-SE to learn the Media Access Control (MAC, Layer 2) addresses of the MLS-enabled router interfaces, check the flowmask of the MLS-RP (explained later in this document), and confirm that the MLS-RP is operational. The MLS-RP sends out multicast "hello" packets every 15 seconds using MLSP; if three of these intervals are missed, then the MLS-SE recognizes that the MLS-RP has failed or that connectivity to it has been lost.

QUESTION 128:

DRAG DROP
Match the correct definition on the right to the switching term on the left.

Answer:



Explanation:
MLS components:
* Multilayer Switching Engine (MLS-SE) - The switching entity that handles the function of moving and rewriting packets.
* Multilayer Switching Route Processor (MLS-RP) - A route switch module or an externally connected Cisco series router with software that supports multilayer switching.
* Multilayer Switching Protocol (MLSP) - This protocol operates between the MLS-SE and MLS-RP to enable multilayer switching.
* MLS Flow - The PFC maintains a Layer3 switching table (the Layer3 MLS cache) for Layer3-switched flows. The cache also includes entries for traffic statistics that are updated in tandem with the switching of packets. After the MLS cache is created, packets identified as belonging to an existing flow can be Layer3 switched based on the cached information. The MLS cache maintains flow information for all active flows. An MLS cache entry is created for the initial packet of each flow. Upon receipt of a packet that does not match any flow currently in the MLS cache; a new IP MLS entry is created.
Note:
IP MLS Flows
Layer 3 protocols, such as IP and Internetwork Packet Exchange (IPX), are connectionless-they deliver every packet independently of every other packet. However, actual network traffic consists of many
end-to-end conversations, or flows, between users or applications. A flow is a unidirectional sequence of packets between a particular source and destination that share the same protocol and transport-layer
information. Communication from a client to a server and from the server to the client are separate flows. For example, Telnet traffic transferred from a particular source to a particular destination comprises a separate flow from File Transfer Protocol (FTP) packets between the same source and destination.
Flows are based only on Layer 3 addresses, which allow IP traffic from multiple users or applications to a particular destination to be carried on a single flow if only the

destination IP address is used to identify a flow.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 219 + 220
http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a008007c8

QUESTION 129:

A new MLS-SE switch is being used on the Certkiller network. What's the definition of a MLS-SE?

A. It is a switch with special MLS IOS.
B. It is a switch with special hardware.
C. It is a switch with special ports.
D. It is a switch with special software.
E. None of the above.

Answer: B

Explanation:
The MLS-SE is a switch with special hardware. For a member of the Catalyst 5000 family, MLS requires that the supervisor have a Netflow Feature Card (NFFC) installed. The Supervisor IIG and IIIG have one by default. In addition, a bare minimum of Catalyst OS 4.1.1 software is also required. Note that the 4.x train is now in General Deployment (GD), or passed rigorous end-user criteria and field-experience targets for stability, so check Cisco's website for the latest releases. IP MLS is supported and automatically enabled for Catalyst 6000 hardware and software with the MSFC/PFC (other routers have MLS disabled by default). Note that IPX MLS and MLS for multicasting may have different hardware and software (Cisco IOS and Catalyst OS) requirements. More Cisco platforms do/will support the MLS feature. Also, MLS must be enabled in order for a switch to be an MLS-SE.

QUESTION 130:

Switch CK1 contains 2 supervisor cards for redundancy. What's true of a Catalyst switch with dual supervisor cards? (Select two)

A. The supervisor engines must be the same model.
B. The active supervisor is selected by priority.
C. The active supervisor controls the system bus.
D. The relevant protocols are active in the standby supervisor.
E. The supervisor engines perform load sharing.

Answer: A, C
Redundant supervisor engines must be of the same type with the same model feature card.
The active supervisor is responsible for controlling the system bus and all line cards.

QUESTION 131:

Switch CK1 is using MLS for switching packets. Which of the following are valid flow masks for MLS-SE? (Select all that apply)

A. source-destination-ip
B. ip-sum
C. ip-bypass
D. destination-ip
E. ip-flow
F. None of the above.

Answer: A, D, E

Explanation:
The three flow masks are as follows:
Destination-IP: The least-specific flow mask. The MLS-SE maintains one MLS entry for each destination IP address. All flows to a given destination IP address use this MLS entry. This mode is used if there are no access lists configured on any of the MLS-RP interfaces.
Source-Destination-IP: The MLS-SE maintains one MLS entry for each source and destination IP address pair. All flows between a given source and destination use this MLS entry regardless of the IP protocol ports. This mode is used if there is a standard access list on any of the MLS-RP interfaces.
IP-flow: The most-specific flow mask. The MLS-SE creates and maintains a separate MLS cache entry for every IP flow. An ip-flow entry includes the source IP address, destination IP address, protocol, and protocol ports. This mode is used if there is an extended access list on any of the MLS-RP interfaces.

QUESTION 132:

What is true about the Multi-layer Switching (MLS) cache?

A. MLS cache entries support unidirectional flows.
B. The MLS-RP stores routing information in the MLS cache.
C. The MLS-SE deletes a cache entry when it detects a TCP FIN ACK
D. The MLS-RP creates MLS cache entries based on known data flows.

Answer: A

Explanation:
An MLS cache entry is created for the initial packet of each flow. A flow is a unidirectional sequence of packets between a particular source and destination that share the same protocol and transport-layer information. Communication from a client to a server and from the server to the client are separate flows. For example, Hypertext

Transfer Protocol (HTTP) Web packets from a particular source to a particular destination are a separate flow from File Transfer Protocol (FTP) file transfer packets between the same pair of hosts.
Incorrect Answers:
B: Routing information is not stored in the MLS cache.
C: The state and identify of the flow are maintained while packet traffic is active; when traffic for a flow ceases, the entry ages out.
D: The MLS-SE, not the MLS-RP creates MLS cache entries.

QUESTION 133:

Which one of the following answer choices describes a hardware-based PDU header rewriting and forwarding based on specific information obtained from multiple OSI layers?

A. Multiplayer switching
B. Cisco express routing
C. Multilayer switching
D. Multilayer routing
E. Router express forwarding

Answer: C

Explanation:
To determine the best path is the primary function of routing protocols, and this can be a CPU-intensive process. Thus, there is a significant performance increase with the offload of a portion of this function to switching hardware. This performance increase is the goal of the MLS feature.
Two of the three major components of MLS are the MLS route processor (MLS-RP) and the MLS switching engine (MLS-SE). The MLS-RP is the MLS-enabled router, which performs the traditional function of routing between subnets/VLANs. The MLS-SE is a MLS-enabled switch, which normally requires a router to route between subnets/VLANs. However, with special hardware and software, MLS-SE can handle the rewrite of the packet. When a packet transverses a routed interface, the change (rewrite) of non-data portions of the packet occurs as the packet heads to the destination, hop by hop.
Confusion can arise here because a Layer 2 device appears to take on a Layer 3 task. Actually, the switch only rewrites Layer 3 information and "switches" between subnets/VLANs. The router is still responsible for standards-based route calculations and best-path determination. You can avoid much of this confusion if you mentally keep the routing and switching functions separate, especially when they are within the same chassis (as with an internal MLS-RP). Think of MLS as a much more advanced form of route cache, with a separation of the cache from the router on a switch. MLS requires both the MLS-RP and the MLS-SE, along with respective hardware and software minimums
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 219

QUESTION 134:

Some Cisco Supervisor Engines have modular uplink ports so that a module can be selected to provide an appropriate level of bandwidth. Which of the following two features are valid on 2-port 1000Base SX or 1000Base LX modular uplink modules? (Select two)

A. 10/100 Autosensing
B. Fast EtherChannel
C. ISL
D. 802.1Q
E. L2 rewrite
F. L3 rewrite

Answer: C, D

Explanation:
Two ways that Ethernet trunking can be implemented are:
* InterSwitch Link (ISL) (Cisco proprietary protocol)
* 802.1q (IEEE standard)
Trunking can only be performed on fast ethernet and Gigabit ethernet links. In this case, either trunking method can be performed over the 2 port Gig E fiber links.
Incorrect Answers:
A: 1000 Base SX and 1000 base LX links are gigabit ethernet, and do not perform the auto-sensing functions that a 10/100 interface performs.
B: Although Gigabit links can be bonded using channeling, the correct term would be gigabit ethernetchannel in this case, not fast EtherChannel.

QUESTION 135:

The Certkiller network needs to pass traffic between VLANs. Which device should be used to accomplish this?

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

Answer: C

Explanation:
A VLAN is a virtual LAN contained within a switch, so for it to pass information into a different VLAN within the same switch it has to leave that switch and re-enter via a router. VLANs contain local traffic only, so in order to reach users in another VLAN the traffic must go through a router or a layer 3 routing processor.

QUESTION 136:

What command would you enter into a Cisco device if you wanted to allow IOS to handle IP datagrams in the Certkiller network with the source routing header option? (Type in the answer below):

Answer: ip source-route

Explanation:
To allow the Cisco IOS software to handle IP datagrams with source routing header options, use the ip source-route global configuration command. To have the software discard any IP datagram containing a source-route option, use the no form of this command.
ip source-route
no ip source-route

QUESTION 137:

You are configuring a Cisco multilayer switch for the Certkiller network. Which command would you use to configure a port to act as a routed interface?

A. ip routing
B. switchport mode trunk
C. no switchport
D. switchport trunk native vlan 1

Answer: C
To turn a switch-port into a router interface, it is simply a matter of turning off the switch-port functionality.
Switch(config)#interface fa 0/1
Switch(config-if)#no switchport

QUESTION 138:

At what state does an HSRP-configured router have to be in to perform packet transfer?

A. Listening
B. Active
C. Standby
D. Queuing
E. Waiting
F. Speaking and listening

Answer: B

Explanation:
At any time, HSRP-configured routers are in one of the following states:
Active-The router is performing packet-transfer functions.
Standby-The router is prepared to assume packet-transfer functions if the active router fails.
Speaking and listening-The router is sending and receiving hello messages.
Listening-The router is receiving hello messages.
Only the active HSRP router actually forwards packets.

QUESTION 139:

Inter-VLAN routing has been implemented in the Certkiller network. In VLAN routing, what are some of the disadvantages of designing a router-on-stick configuration? (Select three)

A. InterVLAN routing cannot be filtered by the router.
B. The router becomes a single point of failure for the network.
C. Routers will not route STP BPDUs.
D. There is a possibility of inadequate bandwidth for each VLAN.
E. Additional overhead on the router can occur.
F. NetFlow Switching is required for InterVLAN accounting.

Answer: B, D, E

Explanation:
A router connected to a switch via a single trunk link is better known as router-on-stick or even a one armed router. Since there's only one router, if that router were to go down there'd be no backup. Since there's only one router, that router would have to handle all the bandwidth of every VLAN so there's a chance it could be overloaded, as with the overhead problems of being responsible for too much.
Because traffic routed between the VLANs traverse a single physical port, there is the potential to not provide for enough bandwidth for a VLAN at any given time.
Inter-VLAN routing also does indeed require additional configuration, management, and overhead.
Incorrect Answers:
A: This is not true since routers can indeed filter traffic that is routed between the VLAN subinterfaces.
C: This is not an advantage. Since BPDU's are local to the VLAN, there is generally no need to route this traffic between the VLANs.
F: This does not apply as a disadvantage to inter-VLAN routing.

QUESTION 140:

Which two statements are true when the extended system ID feature is enabled?
Select two.

A. THE BID is made up of the bridge priority value (two bytes) and bridge MAC address (six bytes).
B. THE BID is made up of the bridge priority value (four bits), the system ID (12 bits), and a bridge MAC address (48 bits).
C. The BID is made up of the system ID (six bytes) and bridge priority value (two bytes).
D. The system ID value is the VLAN ID (VID).
E. The system ID value is unique MAC address allocated from a pool of MAC addresses assigned to the switch or module.
F. The system ID value is a hex number used to measure the preference of a bridge in the spanning-tree algorithm.

Answer: B, D
Expklanation:
According to Cisco white paper:Extended System ID
A 12-bit extended system ID field is part of the bridge ID. Chassis that support only 64 MAC addresses always use the 12-bit extended system ID. On chassis that support 1024 MAC addresses, you can enable use of the extended system ID. STP uses the VLAN ID as the extended system ID. See the "Enabling the Extended System ID" section.

QUESTION 141:

On a multilayer Catalyst switch, which interface command is used to convert a Layer 3 interface to Layer 2 interface?

A. switchport
B. no switchport
C. switchport mode access
D. switchport access vlan vlan-id

Answer: A

QUESTION 142:

Across the Certkiller LAN, Root Link Query messages are being transmitted. Which technology uses a Root Link Query Bridge Protocol Data Unit (BPDU)?

A. BackboneFast
B. PortFast
C. UplinkFast
D. STP standard
E. None of the above

Answer: A

Explanation:
If the local switch has blocked ports, BackboneFast begins to use the Root Link Query

(RLQ) protocol to if upstream switches have stable connections to the Root Bridge.
Reference: Cisco Press CCNP BCMSN, ISBN 1-58720-077-5, by David Hucaby - Chapter 10 Page 254

QUESTION 143:

You are the network administrator at Certkiller and are overlooking a Cisco switch with a redundant power supply of the same wattage. What is the total power available to the switch when both of the power supplies are operating normally? (Select all that apply.)

A. Total power of one supply.
B. Total combined power of both supplies.
C. Total power is the sum of one-half of total power of both supplies.
D. Total power required is shared nearly equally by both supplies.

Answer: C, D

Explanation:
Specifying the redundant keyword enables redundancy. In a redundant configuration, the total power drawn from both supplies is at no time greater than the capability of one supply. If one supply malfunctions, the other supply can take over the entire system load. When you install and turn on two power supplies, each concurrently provides approximately half of the required power to the system. Load sharing and redundancy are enable automatically; no software configuration is required
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e

---

QUESTION 144:

What is the purpose of MST, according to the IEEE 802.1s standard?

A. It is the spanning-tree implementation used by non-Cisco 802.1Q switches.
B. It runs a separate instance of STP for each VLAN.
C. It allows a VLAN bridge to use multiple spanning trees to prevent Layer 2 loops.
D. It creates a single loop-tree structure that spans the entire Layer 2 network.

Answer: C

Explanation:
IEEE 802.1s MST Overview
MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This new architecture provides multiple forwarding paths for data traffic and enables load balancing.

Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).
In large networks, you can more easily administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanningtree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an MST region.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e

---

QUESTION 145:

Which of the following port states are classified in IEEE 802.1w RSTP (Rapid Spanning Tree Protocol)?

A. Listening, Learning, Forwarding, Blocking, Disabled
B. Learning, Forwarding, Discarding
C. Listening, Forwarding, Active, Blocking
D. Learning, Active, Block

Answer: B

Explanation:
There are only three port states left in RSTP, corresponding to the three possible operational states. The 802.1d states disabled, blocking, and listening have been merged into a unique 802.1w discarding state.
RSTP Port StatesThe port state controls the forwarding and learning processes and provides the values of discarding, learning, and forwarding. Table15-4 provides a comparison between STP port states and RSTP port states.Table15-4 Comparison Between STP and RSTP Port StatesOperational Status STP Port State RSTP Port State Port Included in Active TopologyEnabled Blocking1 Discarding2 NoEnabled Listening Discarding NoEnabled Learning Learning YesEnabled Forwarding Forwarding YesDisabled Disabled Discarding No1IEEE 802.1D port state designation.
2 IEEE 802.1w port state designation. Discarding is the same as blocking in RSTP and MST.Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/spantree.htm#wp1063598

QUESTION 146:

Is the following statement True or False?
Unidirectional links frequently causes bridging loops.

A. True

B. There is not enough information to determine
C. False

Answer: A

Explanation:
According to Cisco:
Unidirectional link is a very frequent cause for a bridging loop. Unidirectional links are often caused by a failure not detected on a fiber link for instance, or a problem with a transceiver. Anything that can lead a link to stay up while providing a one-way communication is very dangerous as far as STP is concerned. In order to prevent the problems associated with this problem, Cisco developed a method to detect and block unidirectional switching links.

QUESTION 147:

The Certkiller network has just procured a new Catalyst 6500 to use on the LAN backbone. On a Catalyst 6500 with dual supervisor modules running Native IOS, which two features provide supervisor module redundancy? (Select two)

A. Route Processor Redundancy (RPR)
B. Route Processor Redundancy Plus (RPR+)
C. Single Route Mode (SRM)
D. Dual Router Mode (DRM)

Answer: A, B

Explanation:
Catalyst6500 series switches support fault resistance by allowing a redundant supervisor engine to take over if the primary supervisor engine fails. RPR supports a switchover time of 2 to 4 minutes and RPR+ supports a switchover time of 30 to 60 seconds. When RPR+ mode is used, the redundant supervisor engine is fully initialized and configured, which shortens the switchover time. The active supervisor engine checks the image version of the redundant supervisor engine when the redundant supervisor engine comes online. If the image on the redundant supervisor engine does not match the image on the active supervisor engine, RPR redundancy mode is used.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800da

---

QUESTION 148:

The Certkiller network is using IGMP version 2 within their IP multicast network. In IGMPv2, how is the designated querier elected?

A. The first router to appear on a subnet is designated.

B. The host that responds first to the election query is designated.
C. The router with the lowest IP address on subnet is designated.
D. The host with the lowest MAC address on a segment is designated.

Answer: C

Explanation:
Unlike IGMP Version 1, in which the DR and the IGMP querier are typically the same router, in IGMP Version 2, the two functions are separated. The DR and the IGMP querier are selected based on different criteria and may be different routers on the same subnet. The DR is the router with the highest IP address on the subnet, whereas the IGMP querier is the router with the lowest IP address.
Note:
When an IGMP querier is configured for a VLAN, the switch sends out IGMP general query messages every 125 seconds and listens for general query messages from other switches. If the switch receives a general query, a querier election starts. A querier election across switches is based either on IP address or MAC address. For an inbound query, if the source IP address is nonzero, the election is based on the IP address, and the switch with the lower source IP address becomes the querier. If the source IP address is zero for an inbound query, then the election is based on the source MAC address, and the switch with the lower MAC address wins the election and becomes the querier. The switch that becomes the nonquerier maintains an "other querier interval" timer. When this timer expires, the switch elects itself as the querier.

QUESTION 149:

What do you have to do in order to configure PIM on router CK1 for IP multicast routing? (Select two)

A. Have CK1 Join a multicast group.
B. Enable CGMP on CK1 .
C. Enable IP multicast routing on CK1 .
D. Configure the TTL threshold on CK1 .
E. Enable PIM on an interface of CK1 .

Answer: C, E
Explanation
PIM stands for (protocol independent multicast) and it can come in sparse mode (PIM SM), dense mode (PIMDM), or sparse dense mode.
To configure CK1 for PIM, first you enable IP multicast routing:
CK1 #ip multicast-routing
Then you Enable PIM on the interface
CK1 #interface type number
CK1 #ip pim sparse-dense-mode

QUESTION 150:

What is true about an Ethernet MAC address that is mapped to a Layer 3 multicast IP address? (Select two)

A. The first 3 bytes of the Ethernet multicast MAC address are 01:00:5E.
B. The last 3 bytes of the Ethernet multicast MAC address are 01:00:5E.
C. When assigning a Layer 3 multicast address, an Ethernet Layer 2 address is automatically generated from the hardcoded MAC address.
D. The multicast address copies the last 23 bits of the IP address into the last 23 bits of the Ethernet multicast MAC address.
E. The Ethernet multicast address assigned the last 24 bites of the MAC address to all Fs.
F. The Ethernet multicast address assigns the first 24 bits of the MAC address to all Fs.

Answer: A, D

Explanation:
The prefix 01-00-5e identities the frame as multicast: the next bit is always 0, leaving only 23 bits for the multicast address. Because IP multicast groups are 28 bits long, the mapping cannot be one-to-one. Only the 23 least-significant bits for the IP multicast group are placed in the frame. The remaining five high-order bits are ignored resulting in 32 different multicast groups, being mapped to the same Ethernet address.
Reference: CCNP Switching Exam Certification Guide: David Hucaby & Tim Boyles, Cisco Press 2001, ISBN 1-58720 000-7; page 345

QUESTION 151:

What was added to IGMP version 3 to enhance it that was not previously available in earlier versions?

A. Membership query message
B. Membership report message
C. Leave group message
D. Source filtering
E. Destination filtering

Answer: D

Explanation:
IGMP Version 3 (IGMPv3) adds support for "source filtering," which enables a multicast receiver host to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. This membership information enables Cisco IOS software to forward traffic only from those sources from which receivers requested the traffic."
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtigmpv3.htm

QUESTION 152:

Switch CK1 has just received a multicast frame. By default, how does a Layer 2 switch handle IP multicast traffic?

A. It blocks multicast traffic on all ports.
B. It delivers multicast traffic to all ports.
C. It delivers multicast traffic only to ports that subscribe to it.
D. It delivers multicast traffic only to clients that are member of a multicast group.

Answer: B

Explanation:
When you take a layer two switch out of the box (default configuration), it will by send out multicast traffic out all ports, because a Layer 2 switch doesn't know where the multi cast is destined to, so it just sends it out all ports and hopes it is received. The default switch configuration treats an IP multicast packet like any other packet. When a switch receives a frame destined for a device that it is unaware of or that is not yet learned, it will forward the data out all ports.

QUESTION 153:

What are the valid defaults for the Fast Switching of IP Multicasts? (Select all that apply)

A. enabled and supported over X.25 encapsulated interfaces
B. enabled by default on all interfaces
C. disabled by default on all interfaces
D. disabled and not supported over X.25 encapsulated interfaces
E. None of the above.

Answer: B, D

Explanation:
Fast switching allows higher throughput by switching a packet using a cache created by the initial packet sent to a particular destination. Destination addresses are stored in the high-speed cache to expedite forwarding. Routers offer better packet-transfer performance when fast switching is enabled. Fast switching is enabled by default on all interfaces that support fast switching. Fast switching of IP multicast packets is enabled by default on all interfaces (including GRE and DVMRP tunnels), with one exception: It is disabled and not supported over X.25 encapsulated interfaces.

QUESTION 154:

Router CK1 is configured for multicast. How would you display PIM information

cached in the routing table of CK1 ?

A. show ip pim [group-name] [mapping]
B. show ip rp [group-name | group-address] [mapping]
C. show ip pim rp [group-name | group-address] [mapping]
D. show ip rp pim [group-name | group-address] [mapping]
E. show ip mroute [Hostname | group-address]
F. None of the above

Answer: E

Explanation:
The "show ip mroute [Hostname | Group]" command is used to display the multicast routing table. The show ip mroute command displays all groups and sources.
The following is sample output from the show ip mroute command for a router operating in sparse mode:
Router# show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
Outgoing interface list:
Ethernet0, Forward/Sparse, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
Outgoing interface list:
Ethernet0, Forward/Sparse, 5:29:15/0:02:57
Incorrect Answers:
A: This is an invalid command
B: This is an invalid command.
C: To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the show ippim rp command. The following is sample output from the show ip pim rp command:
Router# show ip pim rp
Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
D: This command is invalid

QUESTION 155:

In the Certkiller IP multicast network, which of the following MAC address corresponds to the multicast IP address of 224.0.1.55?

A. 00-00-00-00-01-55
B. 00-01-E0-00-01-37
C. E0-00-01-37-FF-FF
D. 01-00-5E-00-01-37
E. None of the above.

Answer: D

Explanation: Once an application determines the class D IP multicast address it will utilize, that address must be mapped into a MAC layer multicast for delivery across any LAN based system. This process is outlined as follows:
Step 1: Using the Class D address, identify the low order 23 bits of the class D address.
Step2: Map those 23 bits into the low order 23 bits of a MAC address with the fixed high order 25 bits of the IANA's IEEE multicast addressing space prefixed by 01:00:5E.
In this example, the 0.1.55 translates to 00-01-37 in hex so when added to the IEEE multicast MAC address of 01-00-5E the end result is 01-00-5E-00-01-37.

QUESTION 156:

In the Certkiller IP multicast network, the multicast IP address 224.0.16.111 translates to which MAC address?

A. 00-01-E0-00-10-6F
B. 01-00-5E-00-10-6F
C. 00-01-5E-00-10-6F
D. 00-00-00-00-10-6F
E. E0-00-10-6F-FF-FF
F. None of the above.

Answer: B

Explanation:
Once an application determines the class D IP multicast address it will utilize, that address must be mapped into a MAC layer multicast for delivery across any LAN based system. This process is outlined as follows:
Step 1: Using the Class D address, identify the low order 23 bits of the class D address.
Step2: Map those 23 bits into the low order 23 bits of a MAC address with the fixed high order bits of the IANA's IEEE multicast addressing space prefixed by 01:00:5E.
In this scenario this translates to 01-00-5E-00-10-6F
Incorrect Answers:
The Multicast MAC prefix is always 01-00-5e.
Reference: Whitepaper, Enterasys LAN Switching, Deploying IP Multicast Switching

Method of assuring globally unique MAC address mappings in an IP multicast environment.

QUESTION 157:

A network administrator at Certkiller assigns a multicast address of 239.255.8.5 to an application running on a device with an Ethernet MAC address of 01.b2.7d.05.f1.80. Which Layer 2 multicast address will this particular device use?

A. 01.00.5e.7f.08.05
B. 01.b2.7d.05.f1.80
C. 01.b2.7d.0a.08.05
D. 01.00.5e.05.f1.80
E. ff.ff.ff.ff.ff.ff

Answer: A

Explanation:
Once an application determines the class D IP multicast address it will utilize, that address must be mapped into a MAC layer multicast for delivery across any LAN based system. This process is outlined as follows:
Step 1: Using the Class D address, identify the low order 23 bits of the class D address.
Step2: Map those 23 bits into the low order 23 bits of a MAC address with the fixed high order bits of the IANA's IEEE multicast addressing space prefixed by 01:00:5E.
In this scenario the lower 23 bits translates to 127.8.5 (leaving out the first bit in 255 leaves us with 127) which translates to 7F-08-05 in hex so the final multicast MAC address is 01-00-5E-7F-08-05.

QUESTION 158:

Which of the following layer-2 hardware addresses is a valid multicast MAC address?

A. 00-00-00-FA-11-67
B. 01-00-E0-56-AE-3C
C. 00-01-E0-AB-B2-C1
D. 01-00-5E-0A-08-CF
E. FF-FF-FF-FF-FF-FF

Answer: D

Explanation:
Media Access Control (MAC) layer addresses within Ethernet are 48 bit addresses. These 48 bits comprise 24 bits for the Organizational Unit Identifier (OUI) and 24 bits for serial number of the card, which becomes the remainder of the unique address.
The address of a multicast group does not relate to a physical device, but rather to a

transient group of devices; therefore, the MAC address format uses a special OUI. The OUI for IPv4 Multicast is 01:00:5E with the Least Significant Bit Most Significant Byte set. Only half of this address space was allocated for IP Multicast. Therefore, all MAC addresses that start with 01-00-5E are multicast MAC addresses.

QUESTION 159:

Which of the following technologies manages layer 2 multicast traffic by configuring Layer 2 LAN interfaces dynamically to forward multicasts only to the interfaces that want to receive it?

A. IGMP
B. IGMP snooping
C. PIM-DIM
D. DVMRP
E. MOSPF

Answer: B

Explanation:
Understanding IGMP Snooping:
In subnets where you have configured either IGMP (see "Configuring IP Multicast Layer 3 Switching") or the IGMP querier (see the "Enabling the IGMP Querier" section), IGMP snooping manages multicast traffic at Layer2 by configuring Layer2 LAN interfaces dynamically to forward multicast traffic only to those interfaces that want to receive it.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800f4

QUESTION 160:

Which of the following multicast address is reserved for sending out to all the hosts on a subnet?

A. 224.0.0.1
B. 224.0.0.2
C. 224.0.0.255
D. 239.0.0.255

Answer: A

Explanation:
224.0.0.1 is the all-hosts group. If you ping that group, all multicast capable hosts on the network should answer, as every multicast capable host must join that group at start-up on all its multicast capable interfaces. Some of the well known IP multicast addresses are displayed in the following table:

Class D Address Purpose
224.0.0.1 All hosts on a subnet
224.0.0.2 All routers on a subnet
224.0.0.4 All DVMRP routers
224.0.0.5 All MOSPF routers
224.0.0.9 Routing Information Protocol (RIP)-Version 2
224.0.1.1 Network Time Protocol (NTP)
224.0.1.2 SGI Dogfight
224.0.1.7 Audio news
224.0.1.11 IETF audio
224.0.1.12 IETF video
224.0.0.13 Protocol Independent Multicasting
Incorrect Answers:
B: The multicast IP address 224.0.0.2is reserved for All Routers on this Subnet
C: 224.0.1.27-224.0.1.255Unassigned
D: 239.0.0.255 does not apply.
Reference:
RFC 1458, Host Extensions for IP Multicasting
RFC 1700, ASSIGNED NUMBERS
http://www.tldp.org/HOWTO/Multicast-HOWTO-2.html

QUESTION 161:

You work as a network administrator at Certkiller and you built an IP multicast domain using PIM.
Your CTO asks you if you know which mode assumes that the number of actual end-users of the multicast traffic is relatively small. How would you respond?

A. PIM-DM
B. PIM-SM
C. PIM-RP
D. CGMP
E. IGMP snooping

Answer: B

Explanation:
PIM-SM stands for protocol independent multicast - spares mode; and it is designed for 'receiver initiated multicast group membership', so it is indeed sparse in its multicasts.
PIM Dense Mode (PIM-DM) uses a fairly simple approach to handle IP multicast routing. The basic assumption behind PIM-DM is that the multicast packet stream has receivers at most locations. An example of this might be a company presentation by the CEO or President of a company. By way of contrast, PIM Sparse Mode (PIM-SM) assumes relatively fewer receivers. An example would be the initial orientation video for new employees.
Reference: http://www.netcraftsmen.net/welcher/papers/multicast02.html

QUESTION 162:

Which of the following statements is true about the default IP multicast settings on a Cisco 5000 switch?

A. IGMP snooping enabled and PIM enabled
B. IGMP snooping enabled and CGMP enabled
C. IGMP enabled and IGMP snooping disabled
D. IGMP snooping enabled and CGMP disabled
E. IGMP snooping disabled and CGMP disabled.

Answer: E

Explanation:
IGMP snooping must be enabled. It is disabled by default. CGMP is also disabled by default as well.
Incorrect Answers
B: CGMP is not enabled by default. It must be manually enabled. Furthermore, you cannot enable CGMP on a switch if IGMP snooping is already enabled on that switch.
C: CGMP is disabled by default.
A, D: IGMP snooping is disabled by default.

QUESTION 163:

You are an administrator at Certkiller . Apprentice Jack tells you that there's a Cisco switching technology that can control multicast traffic so it's only delivered to the switch ports that are enabled as multicast clients. Which technology is she talking about?

A. PIM
B. VTP
C. IGMP
D. CGMP

Answer: D

Explanation:
The key to this question lies with the fact that we are looking for a switching technology.
Cisco Group Management Protocol (CGMP) is a Cisco Proprietary protocol which enables IP multicasting at layer 2 on Cisco's Catalyst switches that do not distinguish between IP multicast data packets and IGMP Report messages, which are both MAC level addressed to the same group address. CGMP performs same tasks as IGMP, and was designed to work with other layer 3 multicast protocols.
Incorrect Answers:
A: PIM (Protocol-Independent Multicast) handles the transmission of multicast packets

to all hosts in the multicast group while preventing loops and wasted bandwidth. The two main PIM modes are sparse and dense. PIM is fundamentally used with routers.
B: VTP is the VLAN Trunking Protocol. It shares VLAN information between switches. It is not used for multicast.
C: Routers use the Internet Group Management Protocol (IGMP) to learn whether members of a group are present on directly attached subnets, and whether or not to forward multicast packets onto those networks. Hosts join multicast groups by sending IGMP report messages.

QUESTION 164:

What is true about CGMP?

A. IGMP snooping must be disabled before you can enable CGMP.
B. PIM must be disabled on an interface where CGMP is enabled.
C. CGMP ensures that all switch ports receive all multicast packets.
D. A CGMP-enabled switch summarizes IGMP information for connected routers.

Answer: A

Explanation:
Before you enable CGMP on a switch, you must disable IGMP snooping if it is enabled. If you try to enable CGMP without first disabling IGMP snooping, an error message is generated.
Note: CGMP (Cisco Group Management Protocol) was first implemented by Cisco to restrain multicast traffic in a layer 2 network.
You can configure the switch to either snoop on Protocol Independent Multicast/Distance Vector Multicast Routing Protocol (PIM/DVMRP) packets or to listen to CGMP self-join packets.
Incorrect Answers:
B: There is no requirement to disable PIM (Protocol Independent Multicast) on the CGMP interface.
C: The idea of CGMP is to restrain multicast traffic.
D: This is not the way it works.
In CGMP the multicast router is considered to be the server since it has done all the work and the layer 2 switch is the CGMP client that uses the router's information to construct its forwarding tables (CAM).
Reference: Configuring Multicast Services
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_2/config/multi.htm

---

QUESTION 165:

CGMP has been configured on switch CK1 . What CGMP information do CGMP-enabled switches and routers exchange?

A. CAM table changes

B. summarized IGMP information
C. multicast join and leave events
D. multicast group to port assignment

Answer: C

Explanation:
When the CGMP-capable router receives an IGMP control packet, it creates a CGMP packet that contains the request type (either join or leave), the multicast group address, and the Media Access Control (MAC) address of the host. The router sends the CGMP packet to a well-known address to which the CGMP-enabled switches listen.
Reference: Configuring Multicast Services
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_2/config/multi.htm

---

QUESTION 166:

You want to configure CGMP on switch CK1 . Which of the following statements is correct for configuring Cisco Group Management Protocol on this switch?

A. PIM must be configured on the CGMP router.
B. Directed broadcasts must be disabled on all CGMP switches.
C. CGMP must be enabled separately for each VLAN where it is desired.
D. The switch must be configured with the ip addresses of all neighboring routers.

Answer: A

Explanation:
Protocol Independent Multicast (PIM) is one of the required elements for multicast configuration. It enables IGMP on the router and allows it to receive and forward traffic on the specified interface. PIM must be enabled on every interface that is to participate in the multicast network.
Incorrect Answers:
B: There is no requirement to disable directed broadcasts.
C: CGMP is enabled for a device, not for each VLAN.
The "set cgmp enable" command is used to enable CMGP support for IP multicast on a switch.
D: This is not required.
Reference: Sybex CCNP 640-504, Enabling PIM on an interface, page 391

QUESTION 167:

The Certkiller network is migrating from IGMP version 1 to IGMP version 2. What message type was added in IGMPv2?

A. Heartbeat
B. Join request

C. Leave report
D. Status report

Answer: C

Explanation: A new IGMP Type was created for the IGMPv2 Leave Group message.
Explicit leave messages were not available in IGMP version 2.
Note: The Leave and Group-Specific messages work together to allow a host to remove itself from the multicast group immediately without interrupting the state of the interface on the multicast router.
Reference: RFC 2236, Internet Group Management Protocol version 2 (IGMPv2), Appendix I - Changes from IGMPv1.

QUESTION 168:

The Certkiller network is migrating from IGMP version 1 to IGMP version 2. Internet Group Management Protocol (IGMP) Version 2 (RFC 2236) has improvements over IGMP (RFC 1112). What was improved in version 2?

A. Leave and join latencies
B. The potential for infinite loops
C. Mapping multicast IP addresses to MAC addresses
D. Lack of coordination between Layer 2 and Layer 3 devices.

Answer: A

Explanation:
The Leave process in version 2 was included to avoid long time-outs that are experienced in version 1. With leave messages, hosts can immediately inform network devices that they no longer wish to receive multicast traffic for a particular session. In version 1, hosts would simply leave and the network devices would need to time out before traffic stopped being forwarded to these hosts.
Reference: RFC2236, Internet Group Management Protocol Version 2

QUESTION 169:

IP multicast is being utilized in the Certkiller network. Which of the following statements best describes the way a multicast session operates?

A. A server sends one copy of each packet to a Class D address.
B. A web server transmits separate content to each client.
C. The application server services each client connection individually.
D. A router sends the protocol information to all clients on the network.
E. None of the above.

Answer: A

Explanation:
IP Multicast uses Class D address as destination. The sending device sends traffic destined to these class D IP addresses. This is used to improve efficiencies, since now a single sender can send traffic to multiple receivers.
Incorrect Answers:
B: Multicast does not include a web server. Furthermore, all selected clients receive the same information.
C: All selected clients receive the same information.
D: Only selected clients receive the information, not every client.

QUESTION 170:

Which of the protocols below has these features?
1. It multicasts information.
2. It is a Cisco switching technology.
3. It forwards multicast packets by using multicast information obtained from routers to improve efficiency.

A. PIM
B. CDP
C. IGMP
D. CGMP

Answer: D

Explanation:
CGMP (Cisco Group Management Protocol) was first implemented by Cisco to restrain multicast traffic in a layer 2 network. CGMP operates between the switch and the router and is able to use information obtained from routers.
Incorrect Answers:
A: You can configure the switch to either snoop on Protocol Independent Multicast/Distance Vector Multicast Routing Protocol (PIM/DVMRP) packets or to listen to CGMP self-join packets. PIM is not Cisco proprietary.
B: CDP (Cisco Discovery Protocol) is used by Cisco devices to learn about the neighboring Cisco devices. It is a layer two technology used to discover neighbour information, such as neighbour IP address, device name, and device type. It is not used for multicasts.
C: IGMP is not a Cisco technology.
References: Configuring Multicast Services
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_2/config/multi.htm
RFC 1112, Host Extensions for IP Multicasting

QUESTION 171:

CGMP has been enabled on switch CK S1 as well as router CKR1. How does Cisco

Group Management Protocol (CGMP) operate?

A. The router broadcasts CGMP frames to all CGMP-enabled interfaces.
B. The router forwards all IGMP control packets to CGMP-enabled switches.
C. The router adds each multicast host MAC address to its CAM table for the destined port.
D. The router forwards CGMP packets to a well-known address to which all CGMP switches listen.

Answer: D

Explanation:
Cisco Group Management Protocol (CGMP) limits the forwarding of IP multicast packets to only those ports associated with IP multicast clients. These clients automatically join and leave groups that receive IP multicast traffic, and the switch dynamically changes its forwarding behavior according to these requests. CGMP was first implemented by Cisco to restrain multicast traffic in a layer 2 network. CGMP frames are Ethernet frames with the destination MAC address: 01-00-0c-dd-dd-dd.
Reference: Multicast in a Campus Network: CGMP and IGMP Snooping
http://www.cisco.com/warp/public/473/22.html#CGMP

QUESTION 172:

How can IGMP snooping affect performance on a Catalyst 2950 switch?

A. Low performance occurs when inbound bandwidth is exceeded.
B. Low performance occurs when outbound bandwidth is exceeded.
C. Low performance occurs when heavy traffic is present.
D. IGMP snooping is performed at wire speed and does not affect switch performance.

Answer: D

Explanation:
With a switching fabric of 13.6 Gbps and a maximum forwarding bandwidth of 13.6 Gbps, Cisco Catalyst 2950 Series switches deliver wire-speed performance on all ports in connecting end stations and users to the company LAN. Cisco Catalyst 2950 Series switches with basic services support performance-boosting features such as Cisco Fast EtherChannel(r) to provide high-performance bandwidth between Cisco Catalyst switches, routers, and servers.
To provide efficient use of resources for bandwidth-hungry applications like multicasts, Cisco Catalyst 2950 Series switches support Internet Group Management Protocol Version 3 (IGMPv3) snooping in hardware. Through the support and configuration of IGMP snooping through the Cisco CMS software, these Cisco Catalyst 2950 Series switches deliver outstanding performance and ease of use in administering and managing multicast applications on the LAN.
The IGMPv3 snooping feature allows the switch to "listen in" on the IGMP conversation

between hosts and routers. When a switch hears an IGMP join request from a host for a given multicast group, the switch adds the host's port number to the group destination address list for that group. And when the switch hears an IGMP leave request, it removes the host's port from the content-addressable memory (CAM) table entry.

QUESTION 173:

CORRECT TEXT
You want to disable CGMP on switch CK1 . Which command would you enter if you had to disable CGMP on a non-IOS command-based switch? (Type in answer below)

Answer: set cgmp disable

Explanation:
Remember, set based commands are used in non-IOS based switches. CGMP was first implemented by Cisco to restrain multicast traffic in a layer 2 network. Because a switch is, by essence, not capable of looking at layer 3 packets, it cannot distinguish an IGMP packet. With CGMP, the router provides the interface between the hosts. The routers "talk" IGMP and the switches "talk" CGMP.
To enable CGMP use the "set cgmp enable" command. To disable is, use the "set cgmp disable" command.

QUESTION 174:

CGMP is being used on the Certkiller network. For CGMP to operate correctly on a switch, what must it be connected to?

A. A switch running EIGRP
B. A switch running IGRP
C. A switch running EGMP
D. A router running IGRP
E. A router running CGMP

Answer: E

Explanation:
CGMP was first implemented by Cisco to restrain multicast traffic in a layer 2 network. Because a switch is, by essence, not capable of looking at layer 3 packets, it cannot distinguish an IGMP packet. With CGMP, the router provides the interface between the hosts. The routers "talk" IGMP, and the switches "talk" CGMP with the routers.

QUESTION 175:

Before an administrator can set up a multicast, you will need to specify an addressing scheme. Which of the following statements is true concerning IP

addressing schemes? (Select all that apply)

A. Class E addresses are reserved
B. Class E addresses are allocated dynamically
C. Class D addresses are allocated dynamically
D. Class D addresses are allocated manually
E. Class D addresses are reserved

Answer: C, E

Explanation: Class D addresses are reserved for multicasts using the range 224.0.0.1-239.255.255.255, but they can also be allocated dynamically. (Statically allocated addresses are reserved for specific protocols that require well known address.)
Reference: CCNP Switching Exam Certification Guide David Hucaby & Tim Boyles, pages 343-344

QUESTION 176:

CGMP is being utilized on the Certkiller network. What kind of information do CGMP-enabled routers and switches exchange?

A. Summarized IGMP information.
B. Multicast group to port assignments.
C. Multicast join and leave events.
D. CAM table changes.

Answer: C

Explanation:
CGMP is based on a client/server model. The router is considered a CGMP server, with the switch taking on the client role. The basis of CGMP is that the IP multicast router sees all IGMP packets and therefore can inform the switch when specific hosts join or leave multicast groups. The switch then uses this information to construct a forwarding table.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 306

QUESTION 177:

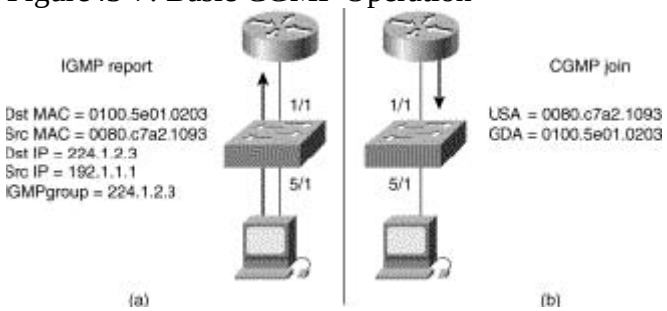
Which protocol(s) prevents switches from flooding multicast traffic out of every port, except the source port?

A. Internet Group Management Protocol Version 1 (IGMPv1)
B. Protocol Independent Multicast (PIM)
C. IP Multicast Routing
D. Cisco Group Management Protocol (CGMP)

E. Internet Group Management Protocol Version 2 (IGMPv2)

Answer: D

Explanation:
CGMPis a Cisco-developed protocol that allows Catalyst switches to leverage IGMP information on Cisco routers to make Layer 2 forwarding decisions. CGMP must be configured both on the multicast routers and on the Layer 2 switches. The net result is that with CGMP, IP multicast traffic is delivered only to those Catalyst switch ports that are interested in the traffic. All other ports that have not explicitly requested the traffic will not receive it.
The basic concept of CGMP is shown in Figure 43-7. When a host joins a multicast group (part A), it multicasts an unsolicited IGMP membership report message to the target group (224.1.2.3, in this example). The IGMP report is passed through the switch to the router for the normal IGMP processing. The router (which must have CGMP enabled on this interface) receives this IGMP report and processes it as it normally would, but in addition it creates a CGMP join message and sends it to the switch.
The switch receives this CGMP join message and then adds the port to its content addressable memory (CAM) table for that multicast group. Subsequent traffic directed to this multicast group will be forwarded out the port for that host. The router port is also added to the entry for the multicast group. Multicast routers must listen to all multicast traffic for every group because the IGMP control messages are also sent as multicast traffic. With CGMP, the switch must listen only to CGMP join and CGMP leave messages from the router. The rest of the multicast traffic is forwarded using its CAM table exactly the way the switch was designed.
Figure43-7: Basic CGMP Operation



CGMP allows for switches to selectively determine which ports to send the IP multicast data, rather than flooding the multicast traffic to all ports except the source port which is the normal multicast behavior of a switch.
Note: IGMP snooping always prevents this as described in this question and would also be a valid answer, had it been a choice in this question.

QUESTION 178:

Your goal is to enable Cisco Group Management Protocol (CGMP) on an interface on your Catalyst 3550 switch. So you connect to the switch and enter interface configuration mode. Which IOS command should you use next?

A. cgmp
B. ip cgmp
C. cgmp enable
D. ip igmp enable cgmp
E. set cgmp enable

Answer: B

Explanation:
In this scenario CGMP is already enabled on the switch. We must enable it on an interface. The ip cgmp interface configuration command is used to enable Cisco Group Management Protocol (CGMP) on an interface. This command is used only on IOS based devices. For native catalyst operation, the "set cgmp enable" command would be used on the switch.

QUESTION 179:

You are tasked with determining the best multicast routing protocol to use on the Certkiller network. Which of the following routing protocols are classified as dense-mode multicast routing protocols? (Select three.)

A. PIM-SM
B. PIM-DM
C. MOSPF
D. OSPF
E. DVMRP

Answer: B, C, E

Explanation:
Dense mode routing protocols include the following:
1. Distance Vector Multicast Routing Protocol (DVMRP)
2. Multicast Open Shortest Path First (MOSPF)
3. Protocol-Independent Multicast Dense Mode (PIM DM)
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 313

QUESTION 180:

Which well-defined routing protocol would a network administrator configure on multicast routers when member routers are widely dispersed?

A. Distance Vector Multicast Routing Protocol (DVMRP)
B. Protocol Independent Multicast Dense Mode (PIM-DM)
C. Multicast Open Shortest Path First (MOSPF)
D. Protocol Indepent Multicast Sparse Mode (PIM-SM)
E. Core-Based Trees (CBT)

Answer: D

QUESTION 181:

Which type of IGMP message is sent when a network client wants to join a multicast group?

A. host member ship query
B. host membership report
C. host membership status
D. host membership notification

Answer: B

QUESTION 182:

When IP multicast is enabled via PIM, which mode uses the flood and prune method?

A. PIM sparse-dense
B. Bidir-PIM
C. PIM-RP
D. PIM-DM
E. PIM-SM

Answer: D

QUESTION 183:

Jitter is causing problems with the VOIP application in the Certkiller network. What causes network jitter?

A. Variable queue delays
B. Packet drops
C. Transmitting too many small packets
D. Compression

Answer: A
Delay variation or jitter is the difference in the delay times of consecutive packets. A jitter buffer is often used to smooth out arrival times, but there are instantaneous and total limits on buffering ability. Any type of buffering used to reduce jitter directly increases total network delay. In general, traffic requiring low latency also requires a minimum variation in latency.
Note: Jitter in Packet Voice Networks:
Jitter is defined as a variation in the delay of received packets. At the sending side,

packets are sent in a continuous stream with the packets being spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, this steady stream can become lumpy, or the delay between each packet can vary instead of remaining constant.

QUESTION 184:

VOIP is being implemented on the Certkiller network. In a properly designed network, what is the maximum amount of time a voice package should spend crossing a network?

A. 90 milliseconds
B. 120 milliseconds
C. 150 milliseconds
D. 240 milliseconds

Answer: C

Explanation:
Delay is the time it takes for VoIP packets to travel between two endpoints and you should design networks to minimize this delay. However, because of the speed of network links and the processing power of intermediate devices, some delay is expected. The human ear normally accepts up to about 150 milliseconds (ms) of delay without noticing problems (the ITU standard recommends no more than 150 ms of one-way delay).
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5014/products_feature_guide09186a00800880e7.html

---

QUESTION 185:

Which of the following network problems would indicate a need to implement QoS features? (Select three)

A. mis-routed packets
B. excess jitter
C. delay of critical traffic
D. packet loss due to congestion
E. data link layer broadcast storms
F. ftp connections unsuccessful

Answer: B, C, D

Explanation:
Loss, jitter, and delay are the three reasons for implementing QoS features on modern networks. Loss is when a packet disappears on a network. Jitter is a timing mismatch between two way traffic, and delay is when a packet takes too long to get somewhere.
Incorrect Answers:

A: This would indicate a routing problem, or packets being "black-holed." QoS would not help in this situation.
E: Broadcast storms indicate a problem on a LAN segment, such as a babbling host, too many hosts, a segment that is too large, a bad application, etc. QoS would not help in this situation.
F. If only FTP sessions were having issues, then the FTP application or FTP server should be corrected. Normally, FTP sessions are not delay sensitive due to the re-transmission nature of TCP and do not require QoS.

QUESTION 186:

Which QoS mechanisms can you use on a converged network to improve VoIP quality? (Select three)

A. The use of a queuing method that will give VoIP traffic strict priority over other traffic.
B. The use of RTP header compression for the VoIP traffic.
C. The proper classification and marking of the traffic as close to the source as possible.
D. The use of 802.1QinQ trunking for VoIP traffic.
E. The use of WRED.

Answer: A, C, E

Explanation:
In order to optimize the quality of VOIP calls, QoS should be implemented to ensure that VOIP traffic is prioritized over other traffic types.
By providing a strict queue for VOIP traffic, you will ensure that voice calls take precedence over the other traffic types.
In order to properly provide for QoS across the network, the voice traffic should be marked to give priority as close to the source as possible. This will ensure that the traffic is prioritized end to end.
Finally, WRED (Weighted Random Early Detection) could be configured to prevent congestion. WRED can be used to selectively drop less important traffic types, instead of dropping the voice packets when links become busy.
Incorrect Answers:
B: Compression can be used to lower the bandwidth required to transmit VOIP calls, but it will not help with improving the voice quality. In general, compression of any kind lowers the quality of VOIP.
D. The trunking method used will have no bearing on the VOIP quality.

QUESTION 187:

The Certkiller is rolling out Cisco's Architecture for Voice, Video and Integrated Data (AVVID). Which of the following choices represent the fundamental intelligent network services in Cisco's AVVID? (Select all that apply.)

A. Quality of Service (QoS)
B. Intelligent platforms
C. Mobility and scalability
D. Security
E. High availability

Answer: A, C, D, E

Explanation:
By creating a robust foundation of basic connectivity and protocol implementation, Cisco AVVID Network Infrastructure addresses five primary concerns of network deployment:
1. High availability
2. Quality of service (QoS)
3. Security
4. Mobility and
5. Scalability
Reference:
http://www.cisco.com/en/US/netsol/netwarch/ns19/ns24/networking_solutions_audience_business_benefit09186

QUESTION 188:

Which of the characteristics below is associated with the (QoS) Integrated Services Model?

A. QoS classified at layer 3 using IP precedence or DSCP.
B. Guaranteed rate service.
C. Implemented using FIFO queues.
D. All traffic has an equal chance of being dropped.

Answer: B

Explanation:
Cisco IOS QoS includes the following features that provide controlled load service, which is a kind of integrated service:
Resource Reservation Protocol (RSVP) can be used by applications to signal their QoS requirements to the router.
Intelligent queuing mechanisms can be used with RSVP to provide the following kinds of services:
Ø Guaranteed Rate Service, which allows applications to reserve bandwidth to meet their requirements. For example, a Voice over IP (VoIP) application can reserve 32 Mbps end to end using this kind of service. Cisco IOS QoS uses weighted fair queuing (WFQ) with RSVP to provide this kind of service.
Ø Controlled Load Service, which allows applications to have low delay and high throughput even during times of congestion. For example, adaptive real-time applications such as playback of a recorded conference can use this kind of service. Cisco IOS QoS

uses RSVP with Weighted Random Early Detection (WRED) to provide this kind of service.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a008007

QUESTION 189:

Which of the following QoS technologies classifies traffic entering a queue and services traffic based on dynamically observed traffic flows?

A. FIFO
B. WFQ
C. Custom Queuing
D. Priority Queuing

Answer: B

Explanation:
WFQ stands for weighted fair queuing. WFQ is one of Cisco's premier queuing techniques. It is a flow-based queuing algorithm that does two things simultaneously: It schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth between high bandwidth flows. By doing this, it can ensure fair treatment for all traffic types, while ensuring that small transmissions are serviced in a timely manner, rather than waiting for a long data transfer to finish.
Incorrect Answers:
A: This is the First In First Out method, which services traffic just as the name implies.
C, D: These methods service the traffic flows based on the configuration parameters. These configured settings are static, and do not change dynamically.
Reference:
http://www.cisco.com/en/US/tech/ CK5 43/ CK5 44/ CK7 18/tech_protocol_home.html

---

QUESTION 190:

Which Cisco strategy employs Storage Networking?

A. content delivery
B. directory service
C. AVVID
D. File service

Answer: C

Explanation:
AVVID - As an element of Cisco AVVID (Architecture for Voice, Video and Integrated Data), Cisco Storage Networking allows customers to adopt a strategy for accessing,

managing and protecting their growing information resources across a consolidated IP, Gigabit Ethernet, Fiber Channel, and optical network infrastructure.
Reference:
http://www.cisco.com/en/US/partners/pr46/pr13/partners_pgm_brochure.html

---

QUESTION 191:

The Certkiller network is using WRED for some QoS functions. Which characteristic best describes weighted random early detection (WRED)?

A. It is well suited for UDP packets because of their connectionless state.
B. It takes advantage of the TCP congestion control mechanism and drops packets selectively based on IP precedence.
C. It should be used in multi-protocol environments where IPX/SPX packet can be dropped instead of UDP packets.
D. It ensures that flows that use the least bandwidth are more likely to have packets dropped.
E. None of the above.

Answer: B

Explanation:
RED and WRED are congestion avoidance mechanisms. Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network and internetwork bottlenecks before it becomes a problem. These techniques are designed to provide preferential treatment for premium (priority) class traffic under congestion situations while concurrently maximizing network throughput and capacity utilization and minimizing packet loss and delay. WRED and DWRED are the Cisco IOS QoS congestion avoidance features.
Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism. Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. WRED is a derivative of RED that also uses TCP's congestion control mechanism.
Incorrect Answers:
A: WRED and RED take advantage of the inherent congestion control mechanisms of TCP, not UDP.
C: WRED is primarily useful only on IP networks, since it takes advantage of TCP functionality.
D: This choice best describes the functionality of weighted fair queuing (WFQ), not WRED.

QUESTION 192:

Which three QoS mechanisms can be configured to improve VoIP quality on a converged network? Select three.

A. the use of a queuing method that will give VoIP traffic strict priority over other traffic
B. the use of RTP header compression for the VoIP traffic.
C. the proper classification and marking of the traffic as close to the source as possible
D. the use of 802.1QinQ trunking for VoIP traffic
E. the use of WRED for the VoIP traffic

Answer: A, C, E

Explanation:
In order to optimize the quality of VOIP calls, QoS should be implemented to ensure that VOIP traffic is prioritized over other traffic types.
By providing a strict queue for VOIP traffic, you will ensure that voice calls take precedence over the other traffic types.
In order to properly provide for QoS across the network, the voice traffic should be marked to give priority as close to the source as possible. This will ensure that the traffic is prioritized end to end.
Finally, WRED (Weighted Random Early Detection) could be configured to prevent congestion. WRED can be used to selectively drop less important traffic types, instead of dropping the voice packets when links become busy.
Incorrect Answers:
B: Compression can be used to lower the bandwidth required to transmit VOIP calls, but it will not help with improving the voice quality. In general, compression of any kind lowers the quality of VOIP.
D. The trunking method used will have no bearing on the VOIP quality.

QUESTION 193:

What is true about a SPAN (switch port analyzer) session?

A. Affects switching traffic on source ports.
B. Associates multiple source interfaces with a single destination interface.
C. Eliminates multiple copies of packets.
D. Associates a source interface with multiple destination interfaces.
E. None of the above.

Answer: B

Explanation:
The Switched Port Analyzer (SPAN) feature, sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. It operates by mirroring information from a source port or multiple source ports, and sending the copied information to the port that is defined as the analyzer port. A single SPAN port can be used to monitor the traffic from multiple source ports.
Incorrect Answers:

A: Traffic on the source port is merely copied, so original traffic is not affected.
C: SPAN can be used to create multiple copies, not eliminate them.
D: Only one port can be configured as the SPAN destination port.

QUESTION 194:

Which of the following statements are true with SPAN? (Select three)

A. A destination port can be a source port.
B. A destination port can participate in only one SPAN session at a time.
C. A destination port can be an EtherChannel group.
D. A source port can be monitored in multiple SPAN sessions.
E. A source port can be an EtherChannel group.
F. A source port can be a destination port.

Answer: B, D, E
When configuring SPAN:
There can only be one destination port, and this destination port can only participate in one SPAN session at a single time. However, multiple SPAN sessions can be configured, and a source port can participate in multiple SPAN sessions.
An EtherChannel does not form if one of the ports in the bundle is a SPAN destination port. If you try to configure this, the switch tells you:
"Channel port cannot be a Monitor Destination Port
Failed to configure span feature"
A port in an EtherChannel bundle can be used as a SPAN source port.
Incorrect Answers:
A, F: A port cannot double as a destination port and a source port. It must be one or the other.
C: The following restrictions apply for ports that have port-monitoring capability:
1. A monitor port cannot be in a Fast EtherChannel or Gigabit EtherChannel port group.
2. A monitor port cannot be enabled for port security.
3. A monitor port cannot be a multi-VLAN port.
4. A monitor port must be a member of the same VLAN as the port monitored. VLAN membership changes are disallowed on monitor ports and ports being monitored.
5. A monitor port cannot be a dynamic-access port or a trunk port. However, a static-access port can monitor a VLAN on a trunk, a multi-VLAN, or a dynamic-access port. The VLAN monitored is the one associated with the static-access port.
6. Port monitoring does not work if both the monitor and monitored ports are protected ports
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015c612.shtml

---

QUESTION 195:

You are a professor at the Certkiller Academy, and a student asks you to describe 'NetFlow traffic flow' to her. How would you respond?

A. It is a sequence of packets between a particular source and destination.
B. It is a uni-directional sequence of packets between a particular source and destination.
C. It is a bi-directional sequence of packets between a particular source and destination.
D. It is a multi-directional sequence of packets between a particular source and destination.

Answer: A

Explanation:
A NetFlow export-enabled device is one that has been configured to operate with CiscoIOS NetFlow Services software in a way that enables the device to export information about traffic flows between communicating end nodes in a network.
For NetFlow data export, traffic flows in a network have the following attributes in common:
1. Source and destination autonomous system (AS) numbers
2. Source and destination IP addresses
3. Source and destination application port numbers
4. Input interfaces
5. IP type of services (ToS)
6. IP protocol
Reference:
http://www.cisco.com/en/US/products/sw/netmgtsw/ps1974/products_installation_guide_chapter09186a0080080

QUESTION 196:

Which of the following SPAN implementations is designed to support source ports, source VLANs, and destination ports across different switches?

A. RVSPAN
B. MSPAN
C. VSPAN
D. RSPAN

Answer: D
RSPAN is an implementation of SPAN designed to support source ports, source VLANs, and destination ports across different switches.
Remote SPAN (RSPAN): Some source ports are not located on the same switch as the destination port. This is an advanced feature that requires a special VLAN to carry the traffic being monitored by SPAN between switches. RSPAN is not supported on all switches, so check the respective release notes or configuration guide to see if it can be used on the switch you are deploying.
Incorrect Answers:
A, B: This is an invalid SPAN type.
C: This is the VLAN-Based SPAN (VSPAN). On a given switch, the user can choose to

monitor all the ports belonging to a particular VLAN in a single command.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008015c612.shtml#topic8
-

QUESTION 197:

You are a CCNP in the midst of configuring a switching solution on a Token Ring network with some Catalyst 5000 series switches and you need to configure SPAN. Which of the following is true regarding the configuration of the token ring port?

A. The source port must not be a single Token Ring port if the SPAN destination port is a Token Ring port
B. There is nothing special to consider
C. The source port must be a single Token Ring port if the SPAN destination port is a non-Token Ring port
D. The source port must be a single Token Ring port if the SPAN destination port is a Token Ring port
E. None of the above.

Answer: D

Explanation:
According to Cisco, follow these guidelines when configuring SPAN:
If the SPAN destination port is a Token Ring port, then the source port must be a single Token Ring port.
In software releases prior to 4.2, if the SPAN destination port is connected to another device, the port always receives incoming packets for the VLAN it is assigned to but does not participate in spanning tree for that VLAN. To avoid creating spanning tree loops, assign the SPAN destination port to an unused VLAN.
In software release 4.2 and later, incoming traffic on the SPAN destination port is disabled by default. You can enable it using the inpkts enable keywords. However, while the port receives traffic for its assigned VLAN, it does not participate in spanning tree for that VLAN. To avoid creating spanning tree loops with incoming traffic enabled, assign the SPAN destination port to an unused VLAN.
You cannot disable the reception of incoming packets on the destination SPAN port (using the inpkts disable keywords) on Token Ring SPAN destination ports.

QUESTION 198:

What is the purpose of a SPAN session on a switch?

A. To identify the destination portion of a MAC source address.
B. To identify the destination of ISL packets on the outbound switch.
C. To identify the port that mirrors traffic to a protocol analyzer.
D. To identify the destination of ISL packets on all other switches.

E. To select network traffic for analysis
F. To identify the destination for the spanning-tree BPDU.

Answer: E

Explanation:
SPAN (Switch Port Analyzer) selects network traffic for analysis by a Catalyst switch Network Analysis Module, a SwitchProbe device, or other RMON probe. SPAN mirrors traffic from one or more source ports (Ethernet, Fast Ethernet, Token Ring, or FDDI) on any VLAN to a destination port for analysis

---

QUESTION 199:

You are a CCNP and are configuring a switching solution with a set based (non IOS) switch. Which command would you enter to disable SPAN? (Type in answer below):

Answer: set span disable

Explanation:
SPAN selects network traffic for analysis by a Catalyst 5000 family Network Analysis Module, a SwitchProbe device, or other RMON probe. SPAN mirrors traffic from one or more source ports (Ethernet, Fast Ethernet, Token Ring, or FDDI) on any VLAN to a destination port for analysis. To disable SPAN, perform this task in privileged mode:
set span disable [dest_mod/dest_port | all]

QUESTION 200:

Switch CK1 has IP accounting enabled. Which command would you enter if you wanted to define filters to control the hosts for which IP accounting information is kept? (Type in answer below)

Answer: ip accounting-list

Explanation:
To define filters to control the hosts for which IP accounting information is kept, use the ip accounting-list global configuration command. To remove a filter definition, use the no form of this command.
"ip accounting-list ip-address wildcard"
"no ip accounting-list ip-address wildcard"

QUESTION 201:

What happens when a trunk port is configured as a SPAN destination port?

A. The SPAN port will only be able to monitor traffic for the native VLAN of the trunk

port.
B. It allows SPAN to monitor traffic for multiple VLANs and encapsulates it on the trunk.
C. The SPAN port will only be able to monitor traffic for a single VLAN that is defined in the SPAN command syntax.
D. A trunk port is not capable of being configured as a SPAN destination port.

Answer: B

QUESTION 202:

What are four basic security measures that should be implemented on every device at every layer of the hierarchical model? Select four.

A. managed remote access
B. password protection
C. security surveillance
D. privilege levels
E. physical security
F. inventory audit

Answer: A, B, D, E

QUESTION 203:

An ISP provides transparent LAN services to interconnect five different Certkiller locations.
What is true regarding this solution? (Select two)

A. Broadcasts are sent to all sites.
B. It is difficult to implement.
C. Routers do not have to peer with each other.
D. There are scalability issues with this solution.

Answer: A, C

Explanation:
Transparent LAN Service (TLS) provides Ethernet connectivity among geographically separated customer locations, creating a VLAN that spans those locations. Like traditional ethernet networks, broadcasts are sent across the network to all locations. Typically, enterprises deploy TLS within a metro area to interconnect multiple enterprise locations. However, TLS also can be extended to locations worldwide. Used this way, TLS converts wide-area connectivity into a VLAN so that the enterprise customer does not need to own and maintain customer premises equipment (CPE) with wide-area interfaces. Customers are freed from the burden of managing-or even knowing anything about-the WAN connection that links their separate LANs. The need for routers can be

eliminated, since the network is one big LAN.
TLS is much less expensive and simpler to implement on Ethernet than on a Frame Relay or ATM network. The lower cost results primarily from lower equipment costs. Cost savings are a primary reason that TLS accounted for more than 63 percent of Metro Ethernet revenue in 2002 and will account for 60.3 percent in 2007, according to IDC.
Another advantage of implementing TLS on Ethernet is that service providers gain the flexibility to provision more bandwidth, and with varying quality-of-service (QoS) capabilities and service-level agreements (SLAs.)
Because TLS is a low-cost service, the service provider can use it as a draw for bundled services, which increase margins and strengthen the customer relationship. Typical value-added services include Ethernet interface to the Internet, storage transport, and data-center connectivity.

QUESTION 204:

On a Catalyst 2924XL, which command would you enter to set the port duplex?

A. duplex
B. set duplex
C. port duplex
D. set port duplex
E. set duplex port

Answer: A

Explanation:
To configure the duplex operation on an interface, use the duplex command. Use the no form of this command to return the system to half-duplex mode.
Command:
duplex {full | half}
no duplex
Syntax Description
full Specifies full-duplex operation.
half Specifies half-duplex operation.
Default is half
Command Modes: Interface configuration
Incorrect Answers:
B, D, E: Since the 2924XL switch uses Cisco IOS, the "set" commands are not used.
C: This is an invalid command.

QUESTION 205:

You need to download a software image into switch CK1 . Which of the following elements are needed to be able to download this image? (Select all that apply)

A. network connection to a TFTP server

B. the File Transfer Protocol
C. the Trivial File Transfer Protocol
D. network connection to a FTP server
E. None of the above

Answer: A, C

Explanation:
You can download system software images to the switch using the Trivial File Transfer Protocol (TFTP). TFTP allows you to download system image files over the network from a TFTP server. Some modules, such as Catalyst 5000 family FDDI and ATM modules, have their own onboard Flash. When you download a software image file, the switch checks the header of the image file to determine the type of software image.

QUESTION 206:

VLAN maps have been configured on switch CK1 . Which of the following actions are taken in a VLAN map that does not contain a match clause?

A. Implicit deny feature at end of list.
B. Implicit deny feature at start of list.
C. Implicit forward feature at end of list
D. Implicit forward feature at start of list.

Answer: A

Explanation:
Each VLAN access map can consist of one or more map sequences, each sequence with a match clause and an action clause. The match clause specifies IP, IPX, or MAC ACLs for traffic filtering and the action clause specifies the action to be taken when a match occurs. When a flow matches a permit ACL entry the associated action is taken and the flow is not checked against the remaining sequences. When a flow matches a deny ACL entry, it will be checked against the next ACL in the same sequence or the next sequence. If a flow does not match any ACL entry and at least one ACL is configured for that packet type, the packet is denied.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_guide_chapter09186a008007f

---

QUESTION 207:

You have been tasked with configuring trunks throughout the Certkiller switched LAN. Which mode must you choose if you want it to be in permanent trunking mode? (Select all that apply)

A. No negotiate

B. On
C. Auto
D. Desirable
E. Off

Answer: A, B

Explanation:
The following table describes the various Trunking modes and their functions:
Ethernet Trunking Modes Mode Function
on Puts the port into permanent trunking mode and negotiates to convert the link into a trunk link. The port becomes a trunk port even if the neighboring port does not agree to the change.
off Puts the port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The port becomes a nontrunk port even if the neighboring port does not agree to the change.
desirable Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to on, desirable, or auto mode.
auto Makes the port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to on or desirable mode. This is the default mode for all Ethernet ports.
nonegotiate Puts the port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

QUESTION 208:

What is a characteristic of assigning a static VLAN membership?

A. VMPS server lookup is required
B. Easy to configure
C. Easy of adds, moves, and changes
D. Based on MAC address of the connected device

Answer: B

Explanation:
Static port VLAN membership on the switch is assigned manually by the administrator on a port-by-port basis.
Characteristics of static VLAN configurations include the following:
1. Secure
2. Easy to configure
3. Straight forward to monitor
4. Works well in networks where moves, adds, and changes are rare.
Incorrect Answers:
A: VMPS server lookups are a function of dynamic VLANs and are not used with

statically assigned VLANs.
C: Moves, adds, and changes, would require a network administrator to change the configuration of the switch every time a change is required.
D: This would describe a function of dynamic VLAN configurations, where the MAC address of the end user determines the VLAN that it belongs in, instead of the physical port.

QUESTION 209:

Static VLANs are being used on the Certkiller network. What is true about static VLAN's?

A. Devices use DHCP to request their VLAN.
B. Attached devices are unaware of any VLANs.
C. Devices are assigned to VLANs based on their MAC addresses.
D. Devices are in the same VLAN regardless of which port they attach to.

Answer: B

Explanation:
LAN port VLAN membership can be assigned manually on a port-by-port basis. When you assign LAN ports to VLANs using this method, it is known as port-based, or static, VLAN membership.
Attached devices will be unaware of any VLANs.
Incorrect Answers:
A: The DHCP service is not involved in VLAN assignment.
C: Devices are not assigned to VLAN based on their MAC addresses. This is a function of dynamic VLANs.
D: Static VLANs are configured on a port by port basis.
Reference: Configuring VLANs
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/121_8aex/swconfig/vlans.htm

---

QUESTION 210:

You are the network administrator at Certkiller and have just applied this VLAN access map on one of your switches:
Router(config)#vlan access-map thor 10
Router(config-access-map)#match ip address net_10
Router(config-access-map)#action forward
Router(config-access-map)#exit
Router(config)#vlan filter thor vlan-list 12-15
What will this configuration result in?

A. All VLAN 12 through 15 IP traffic matching net_10 is forwarded and all other IP packets are dropped.
B.

IP traffic matching net_10 is dropped an all other IP packets are forwarded to VLANs 12 through 15.
C. IP traffic matching vlan-list 12-15 is forwarded on all other IP packets are dropped.
D. All VLAN 12 through 15 IP traffic is forwarded, other VLAN IP traffic matching net_10 is dropped.

Answer: A

Explanation:
* vlanaccess-map thor 10 Defines the VLAN access map. Optionally, you can specify the VLAN access map sequence number.
* matchip address net_10 Configures the match clause in a VLAN access map sequence.
* actionforward Configures the action clause in a VLAN access map sequence.
* vlanfilter thor vlan-list 12-15 Applies the VLAN access map to the specified VLANs.
VLAN access maps can be applied to VLANs.
Each VLAN access map can consist of one or more map sequences, each sequence with a match clause and an action clause. The match clause specifies IP, IPX, or MAC ACLs for traffic filtering and the action clause specifies the action to be taken when a match occurs. When a flow matches a permit ACL entry, the associated action is taken and the flow is not checked against the remaining sequences. When a flow matches a deny ACL entry, it will be checked against the next ACL in the same sequence or the next sequence. If a flow does not match any ACL entry and at least one ACL is configured for that packet type, the packet is denied.
To use access-control for both bridged and routed traffic, you can use VACLs alone or a combination of VACLs and ACLs. You can define ACLs on the VLAN interfaces to use access-control for both the input and output routed traffic. You can define a VACL to use access-control for the bridged traffic.
Reference:
http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_chapter09186a00801611

QUESTION 211:

When configuring a VLAN for dynamic membership; which of the following guidelines NOT required?

A. Configure a VMPS server
B. Turn off trunking on the port
C. Turn off 802.1x port security
D. Configure the spanning-tree PortFast feature
E. All of the above are required for dynamic VLAN configuration

Answer: C
Reference:

Explanation:
Turning port security on or off is not necessary for enabling dynamic VLANs.
These guidelines and restrictions apply to dynamic port VLAN membership:
1. You must configure VMPS before you configure ports as dynamic.
2. When you configure a port as dynamic, spanning-tree PortFast is enabled automatically for that port. Automatic enabling of spanning-tree PortFast prevents applications on the host from timing out and entering loops caused by incorrect configurations. You can disable spanning-tree PortFast mode on a dynamic port.
3. If you reconfigure a port from a static port to a dynamic port on the same VLAN, the port connects immediately to that VLAN. However, VMPS checks the legality of the specific host on the dynamic port after a certain period.
4. Static secure ports cannot become dynamic ports. You must turn off security on the static secure port before it can become dynamic.
5. Static ports that are trunking cannot become dynamic ports. You must turn off trunking on the trunk port before changing it from static to dynamic.

QUESTION 212:

What is true about access control on bridged and routed VLAN traffic? (Select three)

A. Router ACLs can be applied to the input and output directions of a VLAN interface.
B. Bridged ACLs can be applied to the input and output directions of a VLAN interface.
C. Only router ACLs can be applied to a VLAN interface.
D. VLAN maps and router ACLs can be used in combination.
E. VLAN maps can be applied to a VLAN interface

Answer: A, B, D
Router ACLs are applied on interfaces as either inbound or outbound.
To filter both bridged and routed traffic, VLAN maps can be used by themselves or in conjunction with router ACLs.
VLAN ACLs, also called VLAN maps, which filter both bridged and routed packets.
VLAN maps can be used to filter packets exchanged between devices in the same VLAN.

QUESTION 213:

Switch Certkiller 1 needs to have a port assigned to an existing VLAN. Which IOS command could you use to assign a switch port to a VLAN?

A. switchport mode access
B. switchport trunk access
C. switchport access vlan
D. switchport vlan

Answer: C

Explanation:
To assign a switchport to the VLAN, you would use the switchport access vlan interface configuration command.
Reference: CCNP Switching Exam Certification Guide: page 104, David Hucaby & Tim Boyles, Cisco Press 2001, ISBN 1-58720 000-7

QUESTION 214:

What's true with VLAN port associations? (Select all that apply)

A. ASIC enhances the performance of the association
B. VLAN membership is based on Port through port-to-VLAN association.
C. Routing table enhances the performance of the association
D. VLAN membership is based on Port through port-to-WAN ID association.

Answer: A, B

Explanation:
ASIC (Application Specific Integrated Circuits), layer 2 switches have ASIC chips to help them with wire speed hardware switching. With ASIC, the performance of this association is very high, and is more desirable than the complex routing table lookup type of operation.
VLAN membership is based on Port through port-to-VLAN association.
Incorrect Answers:
C: Routing tables are not consulted when transferring VLAN traffic since VLANs are handled at layer 2 and routing occurs at layer 3.
D: VLAN associations deal with layer two VLANs, not layer 3 WAN IDs.

QUESTION 215:

Which Cisco switch command would you use to map VLANs 10 to 20 to MST instance 1?

A. Switch(config)#vlan 10-20 instance 1
B. Switch(config)#instance 1 vlan 10-20
C. Switch(config-mst)#vlan 10-20 instance 1
D. Switch(config-mst)#instance 1 vlan 10-20
E. None of the above

Answer: D

Explanation:
Beginning in privileged EXEC mode, follow these steps to specify the MST region configuration and enable MSTP. This procedure is required.
Command Purpose
Step1 configure terminal Enter global configuration mode.

Step2 spanning-tree mst configuration Enter MST configuration mode.
Step3 instance instance-id vlan vlan-range Map VLANs to an MST instance.
For instance-id, the range is 1 to 15.
For vlan vlan-range, the range is 1 to 4094.
When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped.
To specify a VLAN range, use a hyphen; for example, instance 1 vlan 1-63maps VLANs 1 through 63 to MST instance 1.
To specify a VLAN series, use a comma; for example, instance 1 vlan 10, 20, 30maps VLANs 10, 20, and 30 to MST instance 1.
Step4 name name Specify the configuration name. The name string has a maximum length of 32 characters and is case sensitive.
Step5 revision version Specify the configuration revision number. The range is 0 to 65535.
Step6 show pending Verify your configuration by displaying the pending configuration.
Step7 exit Apply all changes, and return to global configuration mode.
Step8 spanning-tree mode mst Enable MSTP. RSTP is also enabled.
Caution
Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.
You cannot run both MSTP and PVST+ or both MSTP and rapid PVST+ at the same time.
Step9 end Return to privileged EXEC mode.
Step10 show running-config Verify your entries.
Step11 copy running-config startup-config (Optional) Save your entries in the configuration file.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps5528/products_configuration_guide_chapter09186a00802

QUESTION 216:

Token Ring VLANs are being used in some locations within the Certkiller network.
What's the default VLAN value on a token ring with default port assignments?

A. VLAN 0
B. VLAN 1
C. VLAN 1003
D. VLAN ON
E. VLAN A
F. None of the above

Answer: C

Explanation:
As a rule on the Catalyst 3900, TrCRFs cannot span separate switches or stacks of

switches. One exception to this rule is the default TrCRF. The default TrCRF can contain ports located on separate switches. By default, the Token Ring VLAN configuration on the Catalyst 3900 and the Catalyst 5000 series Token Ring modules has all ports assigned to the default TrCRF (1003). In turn, this default TrCRF is associated with the default TrBRF (1005), which can span switches via ISL. If a user does not configure the ports of a Token Ring module to be associated with a new TrCRF, traffic is passed between the default TrCRFs located on separate switches that are connected via ISL.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/trsrb2/vlan.htm

---

QUESTION 217:

Which Cisco IOS command assigns a Catalyst switch port to VLAN 10?

A. switchport mode vlan 10
B. switchport trunk vlan 10
C. switchport access vlan 10
D. switchport mode access vlan 10

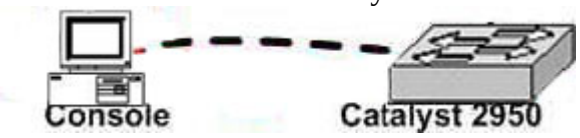
Answer: C

Explanation:
Switchport access:
Use the switchport access interface configuration command to configure a port as a static-access port. The port operates as a member of the configured VLAN.
Use the no form of this command to reset the access mode to the default VLAN for the switch.
Syntax
switchport access vlan vlan-id
no switchport access vlan vlan-id
Syntax Description
vlan vlan-id
ID of the VLAN. Valid IDs are from 1 to 1005. Do not enter leading zeroes.
Defaults
All ports are in static-access mode in VLAN 1.
Command Modes
Interface configuration.
Usage Guidelines
An access port can be assigned to only one VLAN.
When the no switchport access vlan form is used, the access mode is reset to static access on VLAN 1.
Example
The following example shows how to assign a port to VLAN 2 (instead of the default VLAN 1):
Switch(config-if)# switchport access vlan 2
You can verify the previous command by entering the show interface interface-id

switchport command in privileged EXEC mode and examining information in the Administrative Mode and Operational Mode rows.

QUESTION 218:

SIMULATION
You are connected to a Catalyst switch via a console cable as shown below:



You work as a systems administrator at the Certkiller .com main office in the greater Toronto area. The number of employees on your floor has exceeded the infrastructure of your current network equipment. Your CTO has ordered a new switch chassis, but it's going to be another 6-8 working days until it arrives. In the meantime you can to connect 24 new workstations to an old Cisco Catalyst 2950, which your junior administrator has just finished erasing, and rebooting (to purge old VLAN information).
Your tasks are to:
* disable VTP
* Ensure that all non-trunking interfaces do not participate in Spanning Tree by default by globally configuring PortFast.
For the following two tasks, you are required to use global commands to configure the ports:
1. Ensure all FastEthernet interfaces are in permanent non-trunking mode.
2. Place FastEthernet interfaces 0/12 through 0/24 in VLAN 20.
Start by clicking on host CertK iA.

Answer:
enable
configure terminal
Switch(config)#vtp mode transparent (disable vtp)
Switch(config)#spanning-tree portfast default (Globally, enable portfast on all ports)
Switch(config)#interface range fa0/1 - 24 (select interfaces)
Switch(config-if)#switchport mode access (set ports for access mode, NOT Trunking)
switch(config)#interface range fa0/12 - 24 (The 4th task is to "Place FastEthernet interfaces 0/12 through 0/24 in VLAN20")
switch(config-if-range)#switchport access vlan 20
switch(config-if-range)#end
exit
Switch(config-if)#interface range fa0/12 - 24 (select interfaces)
Switch(config-if)#switchport access vlan 20 (assign ports to vlan 20)
end
copy running-config startup-config (save configuration)

QUESTION 219:

You are the network administrator of a network with the active VLANs: 1, 2, 3, 4, 10, 20, and 50. However, you only need to carry VLANs 1,2,10 and 20 on a trunk. Which of the following commands should you use to fulfil this requirement? (Select all that apply.)

A. switchport trunk allowed vlan remove 3,4,50
B. switchport trunk allowed vlan except 3,4,50
C. switchport trunk allowed vlan except 1,2,10,20
D. switchport trunk allowed vlan add 1,2,10,20
E. switchport trunk disallowed vlan remove 3,4,50
F. switchport trunk disallowed vlan add 3,4,50

Answer: A, D

Explanation:
switchporttrunk allowed vlan vlan_list
The vlan_list format is all | none | [add | remove | except] vlan_atom[,vlan_atom...], where:
* all specifies all VLANs from 1 to 4094. This keyword is not supported on commands that do not permit all VLANs in the list to be set at the same time.
* none indicates an empty list. This keyword is not supported on commands that require certain VLANs to be set or at least one VLAN to be set.
* add adds the defined list of VLANs to those currently set, instead of replacing the list.
* remove removes the defined list of VLANs from those currently set, instead of replacing the list.
* except lists the VLANs that should be calculated by inverting the defined list of VLANs.
* vlan_atom is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps663/products_command_reference_chapter09186a008014

QUESTION 220:

Is the following statement True or False?
For each VLAN, if all switches are configured with the default priority, the switch with the highest MAC address in the VLAN will become the root switch.

A. There is not enough information to determine
B. False
C. True

Answer: B

Explanation:
For each VLAN, the switch with the highest bridge priority (the lowest numerical

priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch.

QUESTION 221:

Is the following statement True or False?
The selection of the root switch is not an important issue.

A. False
B. True
C. There is not enough information to determine

Answer: A

Explanation:
The selection of the root switch for a particular VLAN is very important. You can choose it, or you can let the switches decide on their own using default values. The second option is risky because there may be sub-optimal paths in your network if the root selection process is not controlled by you.
Before configuring STP, you need to select a switch to be the root of the spanning-tree. It does not necessarily have to be the most powerful switch ; it should be the most centralized switch on the network. All dataflow across the network will be from the perspective of this switch. It is also important that this switch be the least disturbed switch in the network. The backbone switches are often selected for this function, because they typically do not have end stations connected to them. They are also less likely to be disturbed during moves and changes within the network.
Reference: http://www.cisco.com/warp/public/473/5.html

QUESTION 222:

When you're building up a VLAN, which of the following are part of the sequence?
(Select all that apply)

A. Assign ports.
B. Create VLAN.
C. Create VLAN naming scheme
D. Configure ports for trunking.
E. Remove the trunk when the trunk is no longer needed.
F. Set the baud rate for ports
G. Verify configuration.

Answer: A, B, D, E, G

Explanation:
D, E: To create VLANs on a Catalyst switch, you must first enable the VLAN Trunking

Protocol (VTP). The switch must be in VTP server or transparent mode to do this. VTP clients can not create VLANs.
B: The next step is to create the VLAN.
A: Once the VLAN is created, the final step is to assign individual ports to the VLAN.
G: After everything is configured, it should be verified.
Incorrect Answers:
C: A VLAN naming scheme isn't necessary because VLANs are numbered by default when they're created. Note that A VTP domain name must be created, but the VLANs themselves are not required to be named.
F: The baud rate doesn't have to be set for ports. Setting baud rate is for out-of-band console connections.

QUESTION 223:

What is true regarding the deployment of a VLAN? (Select all that apply)

A. All VLAN hosts are members of the same subnet domain
B. All VLAN hosts are members of the same IP domain
C. All VLAN hosts are members of the same broadcast domain
D. We use VLANs to establish separate broadcast domains to enjoy efficient bandwidth utilization

Answer: A, B, C, D

Explanation:
VLAN's are virtual LAN's and share the same characteristics. Devices on them belong to the same broadcast domains, and they are used for the sake of providing more efficient bandwidth utilization.
VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. All members of a VLAN belong to the same IP subnet.

QUESTION 224:

Switch CK1 is running the Catalyst OS software. What do have to do to create an Ethernet VLAN on CK1 ? (Select all that apply)

A. set vlan vlan_num [name name] [said said] [mtu mtu] [translation vlan_num]
B. set vlanID vlan_num [name name] [said said] [mtu mtu] [translation vlan_num]
C. Go into interface mode
D. set vlanint vlan_num [name name] [said said] [mtu mtu] [translation vlan_num]
E. Go into privileged mode

Answer: A, E

Explanation:

The "set vlan vlan-name" command is used to configure VLANs on CAT OS switches. In order to make any configuration changes to these switches, you must first be in privileged enable mode.
Incorrect Answers:
B, D: These are invalid commands that are using the wrong syntax.
C: In switches running CAT OS, there is no interface configuration mode. All configuration commands are done from the global configuration mode.

QUESTION 225:

What does Cisco recommend you use VLAN 1 for on a switch? (Select two)

A. security
B. load balancing
C. troubleshooting
D. management

Answer: C, D

Explanation:
The default VLAN in a switch for all ports is VLAN 1. It is recommended to create other VLANs within the switch and assign user ports to these new VLANs. However, VLAN 1 should be kept for troubleshooting and management purposes.
Incorrect Answers:
A: Since VLAN 1 is the default VLAN assigned to all ports, it is recommended that users be placed in different VLANs for security purposes. If a user tries to gain unauthorized access into the network, VLAN 1 will be the first VLAN that this user will try to use.
B: The use of VLANs alone will not provide for any load balancing functionality.

QUESTION 226:

Exhibit
switchportmode access
switchportport-security
switchportport-security maximum 2
switchportport-security mac-address 0002.0002.0002
switchportport-security vialoation shutdown
Give the switch interface configuration in the exhibit, what happens when a host with the MAC address of 0003.0003.0003 is directly connected to the switch port?

A. The port will shut down.
B. The host will be allowed to connect.
C. The host will be refused access.
D. The host can only connect through a hub/switch where 0002.0002.0002 is already connected.

Answer: B

QUESTION 227:

In a static VLAN environment, how does a host join a VLAN?

A. It must be assigned to a VLAN dynamically by the VLAN server.
B. It automatically assumes the VLAN of the port.
C. It will assigned to a VLAN based on the username.
D. It will automatically be assigned a VLAN based on its MAC address.

Answer: B

QUESTION 228:

You work as a technician at Certkiller .com. You map VLANs 10 through 20 to MST instance 2.
How will this information be propagated to all appropriate switches?

A. Information will be carried in the RSTP BPDUs.
B. It will be propagated in VTP updates.
C. Information is stored in the Forwarding Information Base and the switch will reply upon query.
D. Multiple Spanning Tree must manually configured on the appropriate switches,.

Answer: D

QUESTION 229:

Assuming you have an IOS based switch; which command would you execute if you wanted to specify IEEE 802.1Q encapsulation on a trunked port?

A. Switch(config-if)#switchport trunk encapsulation dot1q
B. Switch(config-if)#switchport encapsulation dot1q
C. Switch(config-if)#switchport trunk encapsulation isl
D. Switch(config)#switchport 0/1 trunk encapsulation isl

Answer: A

Explanation:
Ethernet Trunk Encapsulation Types:
1. switchporttrunk encapsulation isl - Specifies ISL encapsulation on the trunk link.
2. switchporttrunk encapsulation dot1q - Specifies 802.1Q encapsulation on the trunk link.
3. switchporttrunk encapsulation negotiate - Specifies that the interface negotiate with

the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface.
The trunking mode, the trunk encapsulation type, and the hardware capabilities of the two connected interfaces determine whether a link becomes an ISL or 802.1Q trunk.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps700/products_configuration_guide_chapter09186a008007f

---

QUESTION 230:

Two Certkiller switches are connected as shown below:

witch CK1(config)#inter fa 0/1
witch CK1#switchport trunk encapsulation dot1q
witch CK1(config-if)#switchport mode trunk

Switch CK2(config)#inter fa 0/1
Switch CK2(config)#switchport trunk encapsulation dot1q
Switch CK2(config-if)#switchport mode trunk

Which statements are true regarding the configuration of the above pair of switches? (Select two)

A. The trunk is currently using the ISL trunking protocol.
B. The trunk is currently using the 802.1q trunking protocol.
C. By default, all VLANs will be transmitted across this trunk.
D. By default, Switch CK1 and Switch CK2 's Fast Ethernet 0/1 port will not generate DTP messages.
E. By default, the trunk can only support one VLAN, and only that single VLAN is transmitted across the trunk.

Answer: B, C

Explanation:
The second line in each configuration (#switchport trunk encapsulation dot1q) proves that B is correct, as dot1q is Cisco IOS for 802.1q trunking.
Since the interface fa/01 is configured (#interface fa 0/1) and the mode is set to trunk (#switchport mode trunk) in both switches, there is no need for dynamic trunking protocol since the trunk is already set. By default, all VLANs will be able to cross the trunk, unless explicitly configured not to do so.

QUESTION 231:

Switches Certkiller 1 and Certkiller 2 are connected as shown in the diagram below:

Use the following output taken from each port
Certkiller 1:
showconfig:
interfaceGigabitEthernet0/1
switchport trunk encapsulation dot1q

switchport mode dynamic auto
no ip address
showinterface gig0/1 switchport:
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Certkiller 2:
showinterface gig0/1 switchport:
Name: Gi0/1
Switchport Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
In accordance with the above exhibit: what's preventing the two switches from trunking on the link between them?

A. There is no IP address denied.
B. noshutdown needs to be entered on the interfaces.
C. Both sides are in auto negotiation mode.
D. ISL should be used instead of 802.1q.
E. Access mode VLAN must be different from native mode VLAN.

Answer: C
According to Cisco table Auto & Auto results in NO trunk formation. At least one end of the trunk should be set to on or desirable in order for the trunk to operate correctly.

QUESTION 232:

You have a Cisco Catalyst 3500XL switch within the Certkiller LAN and you want to configure a trunk port on it. Which IOS command should you issue?

A. Switch(config)#vtp mode
B. Switch(config-if)#set trunk
C. Switch(config-if)#encapsulation
D. Switch(config-if)#switchport trunk encapsulation

Answer: D

Explanation:

The switchport trunk encapsulation command is used to specify the trunk encapsulation mode for a port.
Note: Ethernet Trunk Encapsulation Types
Encapsulation Function
switchporttrunk encapsulation isl Specifies ISL encapsulation on the trunk link.
switchporttrunk encapsulation dot1q Specifies 802.1Q encapsulation on the trunk link.
switchporttrunk encapsulation negotiate Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface.
Note: Syntax: set trunk mod/port {on | off |desirable | auto | nonegotiate}[vlans][isl | dot1q | negotiate]
Incorrect Answers:
A: VTP can run in three modes: server, client, and transparent. The vtp mode command is used to set the VTP mode.
B: The set trunk command to configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks.
C: The encapsulation command would only list is used to specify the encapsulation of the VLAN.

QUESTION 233:

The Certkiller network is using 802.1Q for all of the trunks. By default, which statement is correct when an IEEE 802.1Q trunk port receives an untagged frame?

A. The frame is considered in the native VLAN and forwarded to the ports associated with that VLAN.
B. The frame is encapsulated and tagged as in the native VLAN.
C. The frame is broadcast on all ports regardless of VLAN association
D. The frame is dropped

Answer: A

Explanation:
The IEEE802.1Q standard is extremely restrictive to untagged frames. The standard provides only a per-port VLANs solution for untagged frames. For example, assigning untagged frames to VLANs takes into consideration only the port from which they have been received. Each port has a parameter called a permanent virtual identification (Native VLAN) that specifies the VLAN assigned to receive untagged frames.
The main characteristics of IEEE802.1Q are as follows:
Assigns frames to VLANs by filtering.
The standard assumes the presence of a single spanning tree and of an explicit tagging scheme with one-level tagging.
Each physical port has a parameter called PVID. Every 802.1Q port is assigned a PVID value that is of its native VLAN ID (default is VLAN 1). All untagged frames are assigned to the LAN specified in the PVID parameter. When a tagged frame is received

by a port, the tag is respected. If the frame is untagged, the value contained in the PVID (native VLAN) is considered as a tag. Untagged frames are then forwarded to the ports associated with this native VLAN.

QUESTION 234:

You have just configured an ISL trunk line over Ethernet media between two Cisco Switches, each switch having identical modules, software revisions, and VLAN configurations. Which of the following variables are NOT necessary for the ISL trunk to operate properly? (Select all that apply)

A. Identical trunk negotiation parameters at each end of the link
B. Identical duplex at each end of the link
C. Identical speed at each end of the link
D. Identical native VLAN parameters at each end of the link

Answer: A, D

Explanation:
In order for a trunk connection to function properly, it is not necessary for the trunking negotiation parameters to be identical. For example, one end could be configured as "on" and the other could be configured for "auto-negotiate" and the trunk would be operational. Similarly, it is not necessary for the native VLAN parameters to be the same at each end.
Incorrect Answers:
B, C: One of the requirements for trunking to work is to have both sides of the trunk agree on the speed and duplex settings. Both sides must be configured with identical speed and duplex settings.

QUESTION 235:

You must configure an ISL trunk between a Catalyst 5000 Switch and a Catalyst 6000 switch.
What parameters have to be identical for an ISL trunk to work properly? (Select two)

A. an identical VTP mode
B. an identical speed/duplex
C. an identical trunk negotiation parameter
D. an identical trunk encapsulation parameter

Answer: B, D

Explanation:
Speed, duplex, and trunk encapsulation have to be identical at each end. If one end of the trunk is configured for ISL encapsulation and the other is set for 802.1Q encapsulation

the trunk will not come up.
Incorrect Answers:
A: The trunk modes have to be compatible. They don't have to be identical.
C: The Trunk negation parameter does not have to be identical. For example, one end could be configured as "on" and the other could be configured for "auto-negotiate" and the trunk would be operational.

QUESTION 236:

An ISL trunk connects switches CK1 and CK2 . What is the numerical range of user-configurable ISL VLANs on these switches?

A. 1-1001
B. 0-4095
C. there is no range
D. 0 - 1000
E. None of the above

Answer: A

Explanation:
The valid range of user-configurable ISL VLANs is 1-1001. The valid range of VLANs specified in the IEEE 802.1Q standard is 0-4095. In a network environment with non-Cisco devices connected to Cisco switches through 802.1Q trunks, you must map 802.1Q VLAN numbers greater than 1000 to ISL VLAN numbers. 802.1Q VLANs in the range 1-1000 are automatically mapped to the corresponding ISL VLAN. 802.1Q VLAN numbers greater than 1000 must be mapped to an ISL VLAN in order to be recognized and forwarded by Cisco switches.

QUESTION 237:

An ISL trunk connects switches CK1 and CK2 . What is true about the Inter-Switch Link (ISL) protocol? (Select two)

A. ISL can be used between Cisco and non-Cisco switch devices.
B. ISL calculates a new CRC field on top of the existing CRC field.
C. ISL adds 4 bytes of protocol-specific information to the original Ethernet frame.
D. ISL adds 30 bytes of protocol-specific information to the original Ethernet frame.

Answer: B, D

Explanation:
B: A second frame check sequence (FCS) field lies at the end of the frame.
D: ISL is an external tagging process: new 26-byte ISL header is added to the original Ethernet frame. A second 4-byte frame check sequence (FCS) field is added at the end of the frame so 30 bytes of total overhead is added.

Incorrect Answers:
A: Cisco's propriety version of frame tagging is ISL. ISL can only be used between Cisco routers.
C: 30 bytes are added to the Ethernet frame, not 4 bytes. 4 bytes are added using 802.1Q encapsulation.

QUESTION 238:

Which of the commands below enables a trunking protocol that appends a four byte CRC to the packet when applied to the Certkiller switch?

A. Switch(config-if)#switchport trunk encapsulation dot1q
B. Switch(config-if)#switchport trunk encapsulation ietf
C. Switch(config-if)#switchport trunk encapsulation fddi
D. Switch(config-if)#switchport trunk encapsulation isl

Answer: D

Explanation:
ISL is made up of three major components: a header, the original Ethernet frame, and a frame check sequence (FCS) at the end. With ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. The 26-byte header containing a 10-bit VLAN ID is added to each frame. In addition, a 4-byte tail is added to the frame to perform a cyclic redundancy check (CRC). This CRC is in addition to any frame checking that the Ethernet frame performs.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 99

QUESTION 239:

Which statement is true regarding the configuration of ISL trunks?

A. All catalyst switches support ISL trunking.
B. A Catalyst switch will report giants if one side is configured for ISL while the other side is not.
C. ISL trunking requires that native VLANs match.
D. A Catalyst switch cannot have ISL and IEEE 802.1q trunks enabled.

Answer: B

Explanation:
The 802.1q tag is 4 bytes; hence the resulting ethernet frame can be as large 1522 bytes. The minimum size of the Ethernet frame with 802.1q tagging is 68 bytes.
ISL frames are the standard MTU used in Ethernet frames, which is 1518 bytes. If one end of the trunk is configured for ISL frames of up to 1518 bytes will be expected on it, while the other end will be sending frames up to 1522 bytes in length. On the ISL configured end, these incoming frames will be considered as giants. This is just one of

the reasons why ISL and 802.1Q are incompatible.
Incorrect Answers:
A: Not every Cisco switch model supports ISL.
C: In ISL, it is not necessary for the native VLANs to match.
D: Although it is true that each end of a trunk should be configured using the same encapsulation types, it is possible for a switch to have an ISL trunk configured on one port and an 802.1Q trunk on another port.

QUESTION 240:

What command would you enter onto a Cisco router if you wanted to add an IP MLS interface to a VTP domain named sales? (Type in the command below)

Answer: mls rp vtp-domain sales

Explanation:
According to the online documentation provided by Cisco:
To add an IP MLS interface to a VTP domain, perform this task in interface configuration mode:
To add an IP MLS interface to a VTP domain: mls rp vtp-domain [domain_name]
Example: This example shows how to add an IP MLS interface to a VTP domain name engineering:
Router(config-if)mls rp vtp-domain engineering

QUESTION 241:

Which interface configuration mode command would you enter if you wanted to assign a route processor interface to a VTP domain on switch CK1 ?

A. mls rp vlan-id domain-name
B. set mls domain domain-name
C. mls rp vtp-domain domain-name
D. set mls vtp-domain domain-name
E. None of the above

Answer: C

Explanation:
The
mls rp vtp-domain command, applied in interface configuration mode, is used to assign a Multilayer Switching (MLS) interface to a specific Virtual Trunk Protocol (VTP) domain on the Multilayer Switching-Route Processor.
Incorrect Answers:
A: The mls rp vlan-id command is used to assign a virtual LAN (VLAN) identification number to an MLS interface.
B, D: There are no such commands.

QUESTION 242:

You have a non IOS switch named CK1 . On this switch you enter the following command:
setvtp domain
What is the purpose of this command?

A. For determining management domain name
B. For enabling VTP pruning.
C. For selecting VTP version.
D. For verifying configuration set.
E. For verifying configuration.

Answer: A

Explanation: Use the set vtp command to set the options for VTP.
set vtp [domain domain_name] [mode {client | server | transparent}] [passwd passwd] [pruning{enable | disable}] [v2 {enable | disable}]
domain domain_name (Optional) Keywords to define the name that identifies the VLAN management domain. The domain_name can be from 1 to 32 characters in length.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_5/cmd_refr/set_v.htm

QUESTION 243:

Switch CK1 is a Cisco Catalyst 3500XL switch. Which VTP command would you use if you wanted to set the management domain name on a Catalyst 3500XL switch?

A. Switch(vlan)#vtp domain domain-name
B. Switch(config)#vtp domain domain-name
C. Switch(vlan)#set vtp domain domain-name
D. Switch(enable) set vtp domain domain-name

Answer: A

Explanation:
The vtp domain name command is used to assign a name to the VTP management domain on a Catalyst 3500XL switch. Furthermore the prompt would look like: Switch(vlan)# on a switch of this type.
Catalyst 2900 and 3500 switches utilize a VLAN database configuration mode for making changes to the VLAN database parameters.
VLAN Database Mode
The VLAN database commands allow you to modify VLAN parameters. Enter the vlan database command to access VLAN database mode:

Switch> vlan database
Switch(vlan)#
From this mode, enter the "vtp domain" command to set the VTP domain name:
vtpdomain
Use the vtp domain VLAN database command to configure the VLAN Trunking Protocol (VTP) administrative domain.
Incorrect Answers:
B: This command would be correct on a 1900 series switch, not on a Catalyst 3500XL switch.
C: The set vtp domain name command must be issued in enable mode.
D: This command would be correct on a Catalyst 5000 switch, not on a Catalyst 3500XL switch.

QUESTION 244:

You need to configure switch CK1 for pruning. Which VTP command would you use if you wanted to allow pruning?

A. show vtp
B. set vtp
C. set vtp domain
D. set vtp pruneeligible
E. None of the above.

Answer: D

Explanation:
Use the set vtp command to set the options for VTP.
set vtp [domain domain_name] [mode {client | server | transparent}] [passwd passwd] [pruning{enable | disable}] [v2 {enable | disable}]
The pruning keyword is used to enable or disable VTP pruning for the VTP domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the set vtp pruneeligible and clear vtp pruneeligible commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_5/cmd_refr/set_v.htm

---

QUESTION 245:

If you have just configured a Catalyst switch to operate in VTP mode, and that switch is configured to not advertise VLAN configuration information. Which VTP mode has been configured on this switch?

A. Client
B. Server

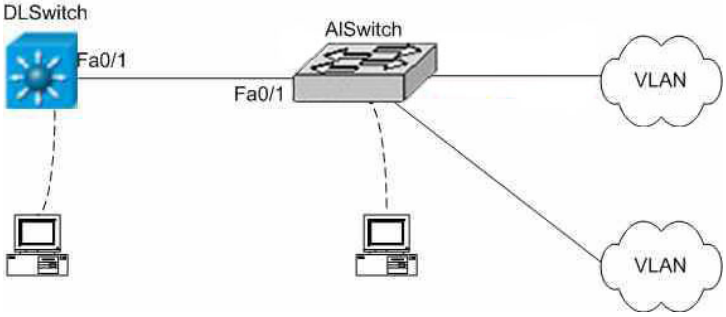
C. Host
D. Transparent
E. Native

Answer: D

Explanation:
You can configure a switch to operate in any one of these VTP modes:
Server-In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.
Client-VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
Transparent
-VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive out their trunk ports.

QUESTION 246:

SIMULATION
The Certkiller network is displayed in the diagram below:



You have just been hired by Certkiller .com to help their main office expand. The main offices have enhanced their wiring closets with some Layer 3 switches. The new distribution layer switch has been installed and a new access layer switch cabled next to it. Your task is to configure the distribution layer and access layer switch with VTP to share VLAN information, then to configure inter-VLAN routing on the distribution layer switch to route traffic between the different VLANs that are configured on the access layer switches.
VTP Domain Distribution
VLAN Ids 20 31
IP Addresses 172.16.71.1/24 172.16.132.1/24
These are your specific tasks:
1. Configure the VTP information with the distribution layer switch as the VTP server

2. Configure the VTP information with the access layer switch as a VTP client
3. Configure VLANs on the distribution layer switch
4. Configure inter-VLAN routing on the distribution layer switch
5. Specific VLAN port assignments will be made as users are added to the access layer switches in the future.
6. All VLANs and VTP configurations are to completed in the global configuration
To configure the switch click on the host icon that is connected to the switch be way of a serial console cable.

Answer:
LAB configuration:
switch#conf t
switch(config)#vtp mode server
switch(config)#vtp domain CISCO
switch(config)#vlan 20
switch(config)#vlan 31
switch(config)#int vlan 20
switch(if-config)#ip add 172.64.20.1 255.255.255.0
switch(if-config)#no shut
switch(if-config)#int vlan 31
switch(if-config)#ip add 192.162.31.1 255.255.255.0
switch(if-config)#no shut
switch(if-config)#exit
switch#ip routing
switch#sh run
switch#copy run start
switch#conf t
switch(config)#vtp mode client
vtp domain CISCO
switch(config)#exit
switch#show run
switch#copy run start
Alternative #1
VTP Domain Distribution
VLAN Ids 20 31
IP Addresses 172.16.16.1/24 172.16.193.1/24
Alternative #12
VTP Domain Distribution
VLAN Ids 30 21
IP Addresses 172.16.203.1/24 172.16.93.1/24

QUESTION 247:

The following commands were entered on a Certkiller switch:
Switch(config)# vtp mode transparent
Switch(config)# vtp version 2

What is the result of these commands?

A. VLAN configuration information is saved in RAM only.
B. VLANs cannot be created, modified or deleted via command line interface.
C. VLAN configuration information received via VTP advertisements are forwarded to other switches within the management domain.
D. VLAN configuration information is synchronized with information within VTP advertisements received from other switches in the management domain.

Answer: C

Explanation:
VTPv2 will allow the switch to be in transparent mode which will forward VTP info. The command series above put the switch in VTP transparent mode. This Certkiller switch does not actively participate in VTP, it doesn't advertise its VLAN configuration to other switches, and when other switches advertise their VLAN configuration it doesn't consider that information. It will, however, pass incoming VLAN information that was received to other switches within the VTP domain.

QUESTION 248:

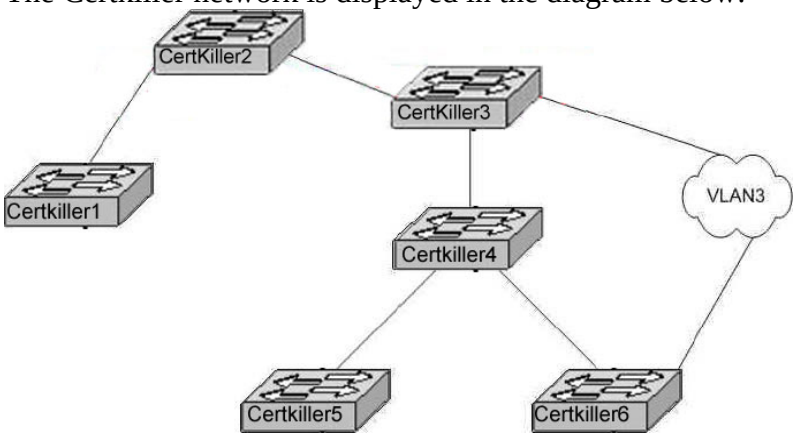
You are a CCNP in the midst of configuring a switching solution on a switch that participates in multilayer switching. What show command would you use to view the MLS interfaces for a specific VTP domain? (Type in the answer below):

Answer: show mls rp vtp-domain

Explanation:
To show MLS interfaces for a specific VTP domain, use the show mls rp vtp-domain EXEC command.
Command: show mls rp vtp-domain [domain-name]

QUESTION 249:

The Certkiller network is displayed in the diagram below:



The network in the above exhibit is configured with VLANs 1,2,3,4, & 5 and 802.1 Q. trunking is enabled between all switches. However, access ports for Certkiller 3 and Certkiller 6 are the only access ports for VLAN 3. What could an administrator do to make sure that other switches don't receive unnecessary broadcast packets destined for VLAN 3, while still allowing all the other VLAN packets to cross?

A. Configure VTP pruning.
B. Configure Certkiller 3 and Certkiller 6 as transparent switches.
C. Configure Certkiller 1, Certkiller 2, Certkiller 4 and Certkiller 5 as transparent switches.
D. Nothing is required.
Only Certkiller 3 and Certkiller 6 will receive VLAN3 packets by default.

Answer: A

Explanation:
VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By configuring VTP pruning, traffic will not flow to switches destined for VLANs that they are not attached to.

QUESTION 250:

You are configuring VTP on a non IOS switch named CK1 , and you enter the following command:
setvtp pruneeligible
What is this command useful for?

A. For determining management domain name
B. For verifying configuration.
C. For enabling VTP pruning.
D. For selecting VTP version.
E. For verifying configuration set

Answer: C

Explanation:
Use the set vtp command to set the options for VTP.
set vtp [domain domain_name] [mode {client | server | transparent}] [passwd passwd] [pruning{enable | disable}] [v2 {enable | disable}]
The pruning keyword is used to enable or disable VTP pruning for the VTP domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the set vtp pruneeligible and clear vtp pruneeligible commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.

Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_5/cmd_refr/set_v.htm

---

QUESTION 251:

While verifying your configuration on the non-IOS based switch named CK1 , you issue the following command:
showtrunk
What is this command useful for?

A. For verifying configuration.
B. For enabling VTP pruning.
C. For verifying configuration set
D. For selecting VTP version.
E. For determining management domain name

Answer: A

Explanation:
Cisco documentation on the use of this command is as follows:
Use the show trunk command to display trunking information for the switch.
show trunk [mod_num[/port_num]] [detail]mod_num (Optional) Number of the module.
/port_num (Optional) Number of the port.
detail (Optional) Keyword to show detailed information about the specified trunk port.

QUESTION 252:

Switch CK1 is configured as a VTP server. What is true when you enable VTP pruning on a VTP server?

A. It is not possible without a root re-election
B. It enables pruning for the entire management domain.
C. It cannot be done on a VTP server
D. It enables pruning for the individual switch.

Answer: B

Explanation:
Enabling VTP pruning on a VTP server enables pruning for the entire management domain. VTP pruning takes effect several seconds after you enable it. By default, VLANs 2 through 1000 are pruning-eligible. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 is always pruning-ineligible; traffic from VLAN 1 cannot be pruned.

QUESTION 253:

One of the configurable VTP commands is displayed below:
Clear vtp pruneeligible vlan_range
What is the purpose of this above command?

A. Verify the VTP pruning configuration.
B. Make specific VLANs pruning-eligible on the device.
C. Make specific VLANs pruning-ineligible on the device.
D. Enable VTP pruning in the management domain.
E. Verify that the appropriate VLANs are being pruned on trunk ports.

Answer: C

Explanation:
This command makes specific VLANs pruning-ineligible on the device. (By default, VLANs 2-1000 are pruning-eligible.)
Note: VLAN 1 is not pruning eligible.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_2/config/vtp.htm

---

QUESTION 254:

When setting up multiple VTP domains, what should be considered in order to maintain VLAN database consistency? (Select two)

A. Do not configure any switches as a VTP server
B. Ensure that all switches not authorized to make changes are in client mode
C. Always configure switches using VTP server mode when adding them to the existing network
D. Allow only one VTP server in each domain so that adding and deleting VLANs can be centralized to one location.

Answer: B, D

Explanation:
B: Switches not authorized to make changes should be run as VTP clients. VTP clients receive information from VTP servers and send and receive updates, but they cannot make any changes.
D: You need at least one server in your VTP domain to propagate VLAN information throughout the domain. You are able to use several VTP servers in a domain. However, only allowing one VTP server would help keep the VLAN database consistent.
Incorrect Answers:
A: Switches can very well be used as VTP servers. VTP server mode is the default for all Catalyst switches.
C: It is more prudent to configure switches using VTP client mode. They will not be able to update information in the VLAN domain database.

QUESTION 255:

VTP is running on the Certkiller network. In which VTP modes can a full list of all VLANs be maintained? (Select two)

A. VTP Bypass
B. VTP Client
C. VTP Transparent
D. VTP Restore
E. VTP Server

Answer: B, E

Explanation:
VTP-capable devices can be configured to operate in the following three modes:
The VTP Server maintains a full list of all VLANs within the VTP domain. Information is stored in nonvolatile random-access memory (NVRAM). The server can add, delete, and rename VLANs.
The VTP Client also maintains a full list of all VLANs. However, it will not store in NVRAM. The client can not add, delete, or rename VLANs. Any changes made must be received from a VTP server advertisement.
The VTP Transparent mode does not participate in VTP. However, it will pass on a VTP advertisement. VLAN, as defined, is only local to the switch and is stored in NVRAM.

QUESTION 256:

You wish to configure VTP on switch CK1 . What do you have to do before you can create a VLAN on a VTP server?

A. The VTP server ID must be cleared
B. The VTP membership list must be refreshed
C. The priority must be cleared
D. The management domain name must be specified

Answer: D

Explanation:
By default, the switch is in VTP server mode and is in the no-management domain state until the switch receives an advertisement for a domain over a trunk link or you configure a management domain. You cannot create or modify VLANs on a VTP server until the management domain name is specified or learned.

QUESTION 257:

What must you do if you wish to configure VTP in secure mode within the Certkiller LAN?

A. Assign a management domain password to the VTP Server in the domain.
B. Assign a management domain password to each switch in the domain.
C. Assign a management domain password to the root switch in the domain.
D. None of the above.

Answer: B

Explanation:
If you configure VTP in secure mode, the management domain will not function properly if you do not assign a management domain password to each switch in the domain. All switches must be configured with the password in order for VTP to function properly in a network.

QUESTION 258:

If you configure a switch as a VTP server offline, then connect it to a network, what could happen to the network?

A. Cause a loss of VLAN information
B. Destabilize the spanning tree
C. Revert to simplex mode
D. Revert to duplex mode
E. Ignore the configuration revision numbers created on the other VTP servers
F. Revert to client mode

Answer: A

Explanation:
When connecting a new switch to your network you can accidentally change your current VLAN database if the new switch has a higher VLAN Trunking Protocol (VTP) revision number. If the newly inserted switch has no VLANs configured and the revision number is higher and is configured as a VTP server, it will override the configuration of the other switches within the network, deleting all of the configured VLANs. To avoid this, you must clear the VTP revision number on the new switch. The easiest way is to change the VTP domain name to "something_else" and back to "your_VTP_domain" on the new switch. This sets the VTP revision number to 0 and you can connect the switch to the network without any problem.

QUESTION 259:

Which of the following are true if you configure a password for VTP? (Select all that apply)

A. It is carried in all summary-advertisement VTP packets
B. It needs to be the same on all switches in the VTP domain

C. It needs to be configured on all switches in the VTP domain
D. It is translated using an algorithm in a 24 bytes word
E. None of the above

Answer: A, B, C

Explanation:
According to the online documentation provided by Cisco:
If you configure a password for VTP, it needs to be configured on all switches in the VTP domain and it needs to be the same password. The VTP password you configure is translated using an algorithm in a 16 bytes word (MD5 value) carried in all summary-advertisement VTP packets.
Incorrect Answers:
D: The algorithm uses a 16 byte word, not 24 bytes.

QUESTION 260:

Is the following statement True or False?
With VTP, if an administrator makes configuration changes centrally on one or more switches, those changes will be automatically communicated to all the other switches on the network.

A. There is not enough information to determine
B. True
C. False

Answer: B

Explanation:
This statement is true. Before you create virtual LANs (VLANs), you must decide whether to use VTP in your network. With VTP, you can make configuration changes centrally on one or more switches and those changes are automatically communicated to all the other switches in the network. Changes made to VTP servers are propagated to all other switches within the VTP domain.

QUESTION 261:

You have to enter a new switch into the existing Certkiller VTP domain without altering the configurations of the systems currently on this domain. Which of the following answer choices describes one of the conditions required to ensure that the new switch will not change the existing VTP domain configuration?

A. The switch must be in client mode.
B. The switch must be in a mode other than the client mode.
C. The VTP domain must not have a password assigned to it.
D. The trunk links must not be configured for ISL

E. None of the above

Answer: A

Explanation:
You can configure a switch to operate in any one of these VTP modes:
Server-In VTP server mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version and VTP pruning) for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.
Client-VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
Transparent-VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2, transparent switches do forward VTP advertisements that they receive out their trunk ports.
Only by using the client or transparent modes can you ensure that the other switches within the domain are left unaffected.

QUESTION 262:

A brand new stand alone Catalyst 3550 switch is being installed. Multiple VLANs will be configured on the switch. What needs to be configured before adding any VLAN to the VLAN database if it is in VTP server mode?

A. VTP pruning
B. VTP domain name
C. VTP version number
D. ISL or IEEE 802.1Q trunking

Answer: B

Explanation:
In order to configure any VLANs and assign ports to them, a VTP server must first have a VTP domain name configured.
Configure the Switch as a VTP Server:
When a switch is configured as a VTP server, you must define a VTP domain before you can create VLANs.
To configure a switch as a VTP server, perform these tasks in privileged mode:
Task Command
Step 1 Assign a name to the VTP management domain. set vtp domain name
Step2 Set the VTP mode. set vtp mode server
Step 3 Verify the VTP configuration. show vtp domain
Reference:

http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008007

QUESTION 263:

Refer to the output shown on switch CK1 below:
VLAN 1 bridge priority set to 8192.
VLAN 1 bridge max aging time set to 20.
VLAN 1 bridge hello time set to 2.
VLAN 1 bridge forward delay set to 15.
Switch is now the root switch for active VLAN 1.
What command would you enter to reproduce this output? (Type in answer below)

Answer: set spantree root 1

Explanation:
According to Cisco:
The default priority for switches is 32768. This command setting means that the switch will be selected as the root switch because it has the lowest priority. This command will set the bridge priority to 8192, unless another switch on the network is already configured with a priority value less that 8192. If this is the case, the priority will be set to one less this value, ensuring that it will become the root switch.
Note: In STP, a lower bridge priority is preferred over a higher value.

QUESTION 264:

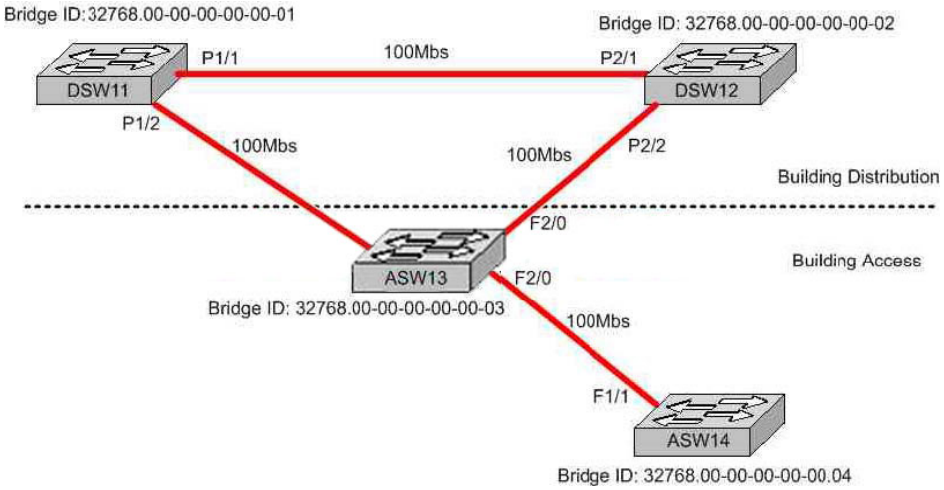
Refer to the output shown on switch CK1 below:
Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.
Spantree ports 4/1-24 fast start enabled.
What command could you enter to reproduce this output? (Type in answer below)

Answer: set spantree portfast 4/1-24 enable

Explanation:
The output shown in this question is the result of the "set spantree portfast" command. This setting should be configured only on ports that are connected to workstations or PCs. Do not enable portfast on any port connected to another switch.

QUESTION 265:

The Certkiller switched LAN is displayed in the diagram below:



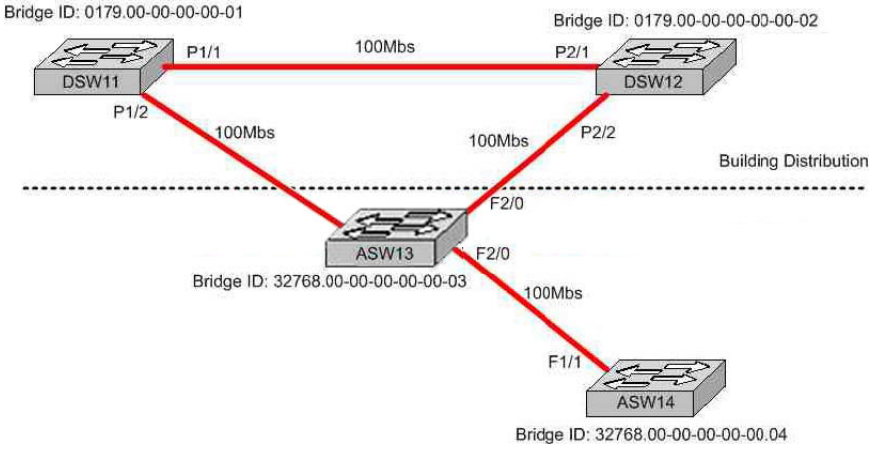
Based on the assumption that STP is enabled on all the switch devices, which of the following statements are true? (Choose two)

A. DSW11 will be elected the root bridge.
B. DSW12 will be elected the root bridge.
C. ASW13 will be elected the root bridge.
D. P1/1 will be elected the nondesignated port.
E. P2/1 will be elected the nondesignated port.
F. F3/0 will be elected the nondesignated port.

Answer: A, F
The root bridge should be placed as close to the core as possible and should be the most centrally located. By default, the switch with the lowest bridge ID will become the root bridge, assuming all other parameters are left as default. This makes DSW11 the root bridge. Also, all ports directly connected to the root bridge will become designated ports, since they are closest to the root bridge. In this case, port F3/0 will become the non-designated port.

QUESTION 266:

The Certkiller switched LAN is displayed below:



Your junior network administrator has just finished installing the above switched network using Cisco 3550s and would like to manipulate the root bridge election. Which switch should he configure as the root bridge and with which command?

A. DSW11(config)# spanning-tree vlan 1 priority 4096
B. DSW12(config)# set spanning-tree priority 4096
C. ASW13(config)# spanning-tree vlan 1 priority 4096
D. DSW11(config)# set spanning-tree priority 4096
E. DSW12(config)# spanning-tree vlan 1 priority 4096
F. ASW13(config)# set spanning-tree priority 4096

Answer: C

Explanation:
Catalyst 3550 is IOS-based switch, so it doesn't use set-based commands, the correct answer should be 'spanning-tree vlan 1 priority 4096' (Answer C).
Note:
Before configuring STP, you need to select a switch to be the root of the spanning-tree. It does not necessarily have a to be most powerful switch; it should be the most centralized switch on the network. All dataflow across the network will be from the perspective of this switch. It is also important that this switch be the least disturbed switch in the network. The backbone switches are often selected for this function, because they typically do not have end stations connected to them. They are also less likely to be disturbed during moves and changes within the network. In this case, switch ASW13 is the most centrally located switch so it should have its bridge priority lowered to become the root.
Note: In the network shown above, if no configuration changes are made, switch DSW11 will become the root by default, since it has the lowest Bridge ID.

QUESTION 267:

Which three items are configured in MST configuration submode? (Select three)

A. Region name
B. Configuration revision number
C. VLAN instance map
D. IST STP BPDU hello timer
E. CST instance map
F. PVST+ instance map

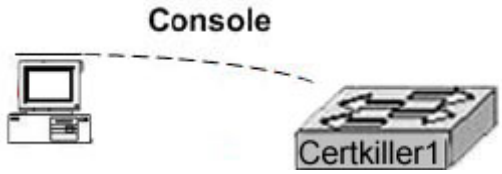
Answer: A, B, C

Explanation:
spanning-treemst configuration:
Use the spanning-tree mst configuration command to enter the MST configuration submode. Use the no form of this command to return to the default MST configuration.

Defaults:
The default value for the MST configuration is the default value for all its parameters:
1. No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).
2. The region name is an empty string.
3. The revision number is 0.
Usage Guidelines:
The MST configuration consists of three main parameters:
1. Instance VLAN mapping (see the instance command)
2. Region name (see the name command)
3. Configuration revision number (see the revision command)

QUESTION 268:

SIMULATION
You are connected to switch Certkiller 1 as displayed in the diagram below:



You work as a network engineer at Certkiller .com. The Certkiller .com Toronto office is installing a temporary Catalyst 3550 in an IDF to connect 24 additional users. To prevent network corruption, it is important to have the correct configuration prior to connecting to the production network. It will be necessary to ensure the switch does not participate in VTP but forwards VTP advertisements received on trunk ports.
All interfaces should transition immediately to the forwarding state of Spanning-Tree due to errors that have been experienced on office computers. Also, configure the user ports (All FastEthernet ports) so that he ports are permanently non-trunking.
You will configure FastEthernet ports 0/12 through 0/24 for users who belong to VLAN 20. Also, all VLAN and VTP configurations are to be completed in global configuration mode as VLAN database mode is being deprecated by Cisco.
You are required to accomplish the following tasks:
1. Ensure the switch does not participate in VTP but forwards VTP advertisements received on trunk ports.
2. Ensure all non-trunking interfaces (Fa0/1 to Fa0/24) transition immediately to the forwarding state of Spanning-Tree.
3. Ensure all FastEthernet interfaces are in a permanent non-trunking mode.
4. Place FastEthernet interfaces 0/12 through 0/24 in VLAN 20

Answer:
Configuration:
switch#configure terminal
switch(config)#vtp mode transparent
switch(config)#spanning-tree portfast default

switch(config)#interface range fa0/1 - 24
switch (config-if-range)#switchport mode access
switch (config-if-range)#end
switch#copy running-config startup-config
Alternative:
switch#configure terminal
switch(config)#vtp mode transparent
switch#interface range fa0/1 - 24
switch (config-if-range)#switchport mode access
switch (config-if-range)#spanning-tree portfast
switch (config-if-range)#end
switch#copy running-config startup-config

QUESTION 269:

If the root bridge fails, configuration BPDUs will no longer be sent. Which STP timer will have to expire before the other switches can actively restore connectivity with topology change procedure of STP?

A. hello timer
B. BPDU timer
C. Forward_delay timer
D. Max_age timer
E. Dead timer
F. Wait timer

Answer: D

Explanation:
Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.
Max age takes into account that the switch at the periphery of the network should not time out the root information under stable condition (that is, if the root is still alive). This is the value that max age needs to take into account the total BPDU propagation delay and the message age overestimate. As such, the formula for max age is as follows:
Max_age
= End-to-end_BPDU_propa_delay + Message_age_overestimate
= 14 + 6
= 20 sec
This explains how IEEE reaches the default recommended value for max age.
Reference: http://www.zyxel.com/support/supportnote/ves1012/app/stp.htm

---

QUESTION 270:

Exhibit

Assuming that VLAN 1 and VLAN 2 traffic is enabled on the above network, what effect will the following command have when entered on port 0/2 on switch Certkiller B?
spanning-tree vlan 1 port-priority 16

A. VLAN 1 traffic will be blocked on Switch Certkiller B port 1/1.
B. VLAN 2 traffic will be blocked on Switch Certkiller B port 1/1.
C. VLAN 2 traffic will be blocked on Switch Certkiller A port 0/2.
D. VLAN 1 and 2 traffic will be blocked on Switch Certkiller A port 0/1.
E. VLAN 1 and 2 traffic will be blocked on Switch Certkiller A port 0/2.

Answer: A

QUESTION 271:

By default, all VLANs will belong to which MST instance when using Multiple STP?

A. MST00
B. MST01
C. the last MST instance configured
D. none

Answer: A

QUESTION 272:

Which MST configuration statement is correct?

A. MST configurations can be propagated to other switches using VTP.
B. After MST is configured on a Switch, PVST+ operations will also be enabled by default.
C. MST configurations must be manually configured on each switch within the MST region.
D. MST configurations only need to be manually configured on the Root Bridge.
E. MST configurations are entered using the VLAN Database mode on Cisco Catalyst switches.

Answer: C
MST configuration must be manually configured on each switch within the MST region.

QUESTION 273:

Exhibit
Certkiller 1#show spanning-tree vlan 200
VLAN200
Spanning tree enabled protocol ieee
Root ID Priority 32968
Address 000c.ce29.ef00
Cost 19
Port 2 (FastEthernet0/2)
Hello time 10 Sec Max Age 20 sec Forward Delay 30 sec
Bridge ID Priority 32968 (priority 32768 sys-id-ext 200)
Address 000c.ce2a.4180
Hello Time 2 sec Max Age 20 Sec Forward Delay 15 sec
Interface Role Sts Cost PrioNbr Type

Fa0/2 Root FWD 19 128.2 P2p
Fa0/3 Altn BLK 19 128.3 P2p
Based on the show spanning-tree vlan 200 output shown in the exhibit, which two statements about the STP process for VLAN 200 are true? (Choose two)

A. BDPUs will be sent out every two seconds.
B. The time spent in the listening state will be 30 seconds
C. The time spent in the learning state will be 15 seconds
D. The maximum length of time that the BPDU information will be saved is 30 seconds.
E. This switch is the root bridge for VLAN 200.
F. BPDUs will be sent out every 10 seconds.

Answer: B, F
Changing the Spanning Tree Protocol Timers
The STP timers (hello, forward delay, and max age) are included in each BPDU. An IEEE bridge is not concerned about its local configuration of the timers value. It will consider the value of the timers contained in the BPDU that it is receiving. Effectively, that means only a timer configured on the root bridge of the STP is important. Obviously, in case you would lose the root, the new root would start to impose its local timer value to the entire network. So, even if it is not required to configure the same timer value in the entire network, it is at least mandatory to configure any timer changes on the root bridge and on the backup root bridge.

QUESTION 274:

You have been promoted to CTO at Certkiller , Inc. and you are looking for ways to increase the efficiency of your network administration. What can your

administrators do to improve the Spanning Tree Protocol's operation?

A. Properly place the Root Bridge to ensure an optimal STP topology.
B. Configure access switches as Root Bridges to ensure optimal workstation access to the network.
C. Load balance on redundant links through the use of technologies such as BackboneFast.
D. Provide for efficient workstation access through the use of BackboneFast.

Answer: A

Explanation:
One of the most important decisions that must be made in the Spanning tree network is the location(s) of the root bridge. Proper placement of the root bridge optimizes the path that is chosen by the Spanning-Tree Protocol.
The root bridge should be placed as close to the core of the network as possible, or in a centrally located position within the LAN.
Incorrect Answers:
B: Core or distribution layer switches should be used as the root of the STP, not access layer switches.
C: Backbone fast does not provide for load balancing. The STP does not provide for any load balancing mechanisms, since its function is to detect and prevent loops.
D: Backbone fast is a Cisco proprietary feature that, once enabled on all switches of a bridge network, can save a switch up to 20 seconds (max_age) when recovering from an indirect link failure. It does not provide for more efficient workstation access.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 151

QUESTION 275:

You are an independent network consultant, and you've just been contracted to troubleshoot a multilayer switched network which is going through some intermittent end-station accessibility issues. The network has a redundant topology and core layer and access layer switches (the root bridge is on one of the core switches). After going through your systematic troubleshooting methodology, you realize that the problem has to do with STP convergence and the accessibility issues depend on the individual ports' STP state. In this scenario you need to decrease STP convergence time. What's the best way of doing it?

A. Enable PortFast on the core switched to accelerate the choice of a new root port.
B. Enable UplinkFast on the WLAN that is having the most accessibility problems.
C. Enable UplinkFast on the wiring closet switches at the edge of the network.
D. Enable PortFast on all IOS based switches that have been configured for bridge priority.

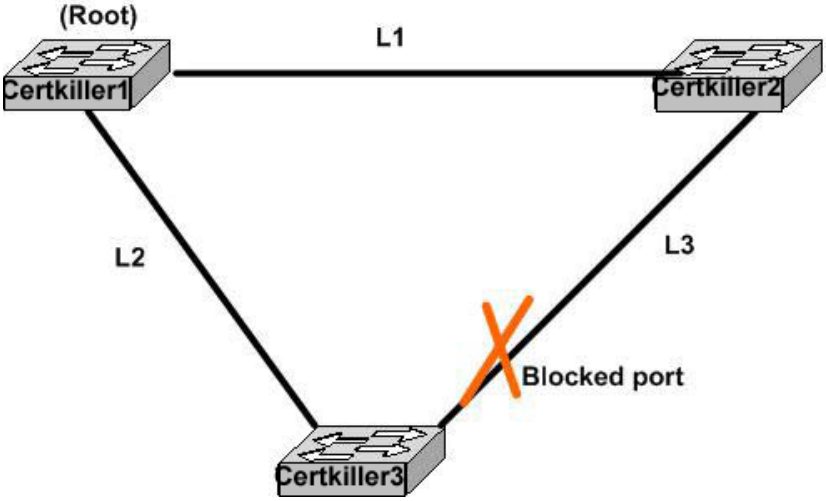
Answer: C

Explanation:
If a switch looses connectivity, it begins using the alternate paths as soon as STP selects a new root port. When STP reconfigures the new root port, other interfaces flood the network with multicast packets, one for each address that was learned on the interface. By using STP UplinkFast, you can accelerate the choice of a new root port when a link or switch fails or when STP reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with normal STP procedures. UplinkFast also limits the burst of multicast traffic by reducing the max-update-rate parameter (the default for this parameter is 150 packets per second). However, if you enter zero, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity.
Note: UplinkFast is most useful in wiring-closet switches at the access or edge of the network. It is not appropriate for backbone devices.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/1216ea2b/scg/swgstp.htm

---

QUESTION 276:

Three Certkiller switches are connected as shown below:



Switch Certkiller 3 is configured with UplinkFast.
If L2 were to fail, how much time will pass before Switch Certkiller 3 activates the port connection to L3?

A. 1-5 seconds
B. 15-20 seconds
C. 30-35 seconds
D. 45 seconds
E. 60 seconds
F. None of the above.

Answer: A

Explanation:

If SwitchC detects a link failure on the currently active link L2 (a direct link failure), UplinkFast unblocks the blocked port on SwitchC and transitions it to the forwarding state immediately, without transitioning the port through the listening and learning states. This switchover takes approximately one to five seconds.

QUESTION 277:

Which of the following commands would you use if you wanted a Layer 2 access port to bypass the listening and learning states and move directly to the forwarding state?

A. spanning-tree uplinkfast
B. spanning-tree port-priority
C. spanning-tree portfast
D. spanning-tree vlan vlan-id reset primary

Answer: C

Explanation:
Spanning Tree PortFast causes an interface configured as a Layer 2 access port to enter the forwarding state immediately, bypassing the listening and learning states. You can use PortFast on Layer 2 access ports connected to a single workstation or server to allow those devices to connect to the network immediately, rather than waiting for spanning tree to converge. If the interface receives a bridge protocol data unit (BPDU), which should not happen if the interface is connected to a single workstation or server, spanning tree puts the port into the blocking state.
To enable PortFast on a Layer 2 access port to force it to enter the forwarding state immediately, perform
this procedure:
Task Command
Step 1 Specify an interface to configure. Switch(config)# interface {{fastethernet | gigabitethernet} slot/ port} | {port-channel
port_channel_number}
Step 2 Enable PortFast on a Layer 2 access port connected to a
single workstation or server.
You can use the no keyword to disable PortFast.
Switch(config-if)# [no] spanning-tree portfast

QUESTION 278:

You are a network troubleshooter and you've been called into the Certkiller to manually put a switch port back into service after it was put into the error disabled state upon receipt of Spanning Tree messages. Which of the following STP features puts a switch port into an error-disabled state when it receives Spanning Tree data messages?

A. BDPU Filtering
B. Root Guard
C. BDPU Guard
D. Port Fast
E. Loop Guard
F. None of the above

Answer: C

Explanation:
Understanding BPDU Guard
The BPDU guard feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.
At the global level, you can enable BPDU guard on Port Fast-enabled ports by using the spanning-tree portfast bpduguard default global configuration command. Spanning tree shuts down ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps5206/products_configuration_guide_chapter09186a008017

QUESTION 279:

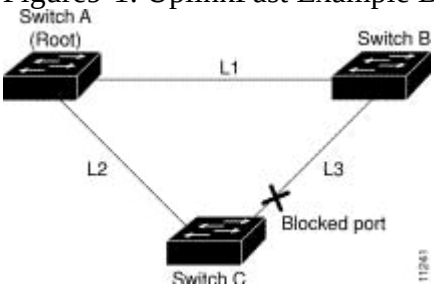
What's true about the UplinkFast feature? (Select two)

A. It must be used with the PortFast feature enabled.
B. When enabled, it is enabled for the entire switch and all VLANs.
C. It should be configured on all switches, including the Root Bridge.
D. When the primary Root Port uplink fails, another blocked uplink can be immediately brought up for use.

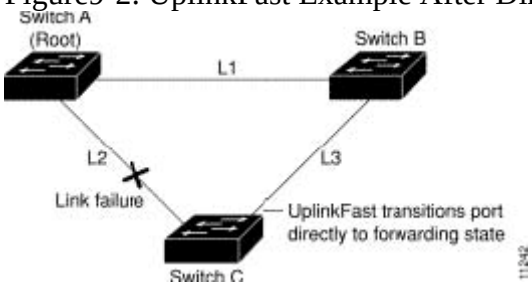
Answer: B, D

Explanation:
UplinkFast provides fast convergence in the network access layer after a spanning-tree topology change using uplink groups. An uplink group is a set of ports (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports (not including self-looped ports). The uplink group provides an alternate path in case the currently forwarding link fails.
NoteUplinkFast is most useful in wiring-closet switches with a limited number of active VLANs. This enhancement might not be useful for other types of applications and should not be enabled on backbone or distribution layer switches.
Figure 9-1 shows an example UplinkFast network topology. SwitchA, the root switch, is

connected directly to SwitchB over link L1 and to SwitchC over link L2. The port on SwitchC that is connected to Switch B over linkL3 is in blocking state.
Figure9-1: UplinkFast Example Before Direct Link Failure



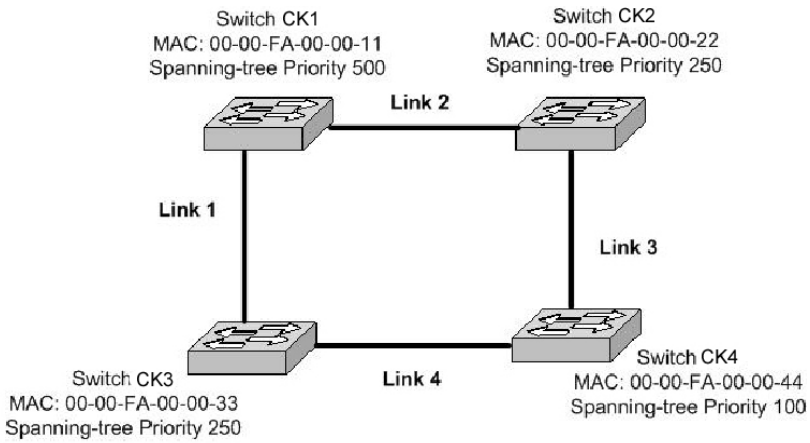
If SwitchC detects a link failure on the currently active link L2 (a direct link failure), UplinkFast unblocks the blocked port on SwitchC and transitions it to the forwarding state immediately, without transitioning the port through the listening and learning states (as shown in Figure 9-2). This switchover takes approximately oneto fiveseconds.
Figure9-2: UplinkFast Example After Direct Link Failure



As soon as the switch transitions the alternate port to the forwarding state, the switch begins transmitting dummy multicast frames on that port, one for each entry in the local EARL table (except those entries associated with the failed root port). By default, approximately 15dummy multicast frames are transmitted per 100milliseconds.
Each dummy multicast frame uses the station address in the EARL table entry as its source MAC address and a dummymulticast address (01-00-0C-CD-CD-CD) as the destination MAC address.
Switches receiving these dummy multicast frames immediately update their EARL table entries for each source MAC address to use the new port, allowing the switches to begin using the new path almost immediately.
If connectivity on the original root port is restored, the switch waits for a period equal to twice the forward delay time plus 5seconds before transitioning the port to the forwarding state in order to allow the neighbor port time to transition through the listening and learning states to the forwarding state.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/stp_enha.htm#xtocid25869

QUESTION 280:

Four Certkiller switches are connected together as shown below:



All the ports in the diagram all have the same spanning-tree cost and they're all configured as access ports. If you wanted to use UplinkFast to improve convergence time after link failure; where should you configure UplinkFast?
A: Switch CK1
B: Switch CK2
C: Switch CK3
D: Switch CK4

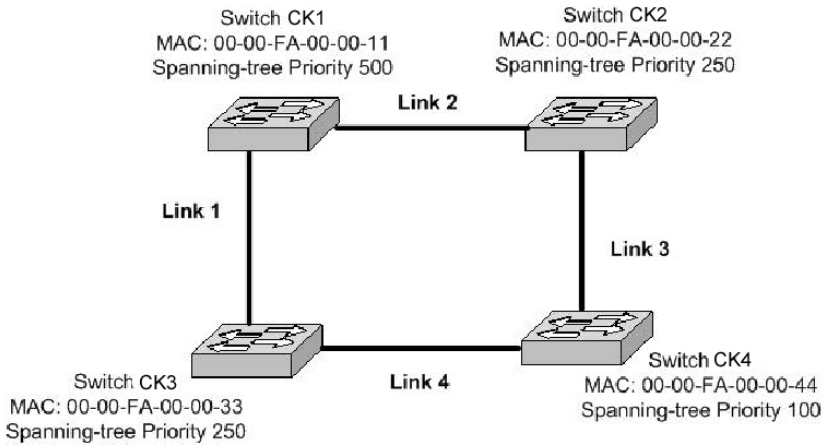
Answer: A

Explanation:
Note: The UplinkFast feature provides fast convergence in the network access layer after a spanning tree topology change by using uplink groups. UplinkFast accelerates the choice of a new root port when a link or switch fails or when STP reconfigures itself. The UplinkFast feature is designed to run in a switched environment when the switch has at least one alternate/backup root port (port in blocking state), that is why Cisco recommends that UplinkFast be enabled only for switches with blocked ports, typically at the access-layer. Do not use on switches without the implied topology knowledge of an alternative/backup root link typically to distribution and core switches in Cisco multilayer design.
In this example, switch CK4 will become the root switch, since it has the lowest bridge priority. Therefore, uplink fast should be configured on switch CK1 .
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK6 21/technologies_tech_note09186a0080094641.shtml#uplink_fast_fa

---

QUESTION 281:

The Certkiller network is depicted in the diagram below:



All the ports are configured as access ports and they all have the same spanning-tree cost. So you want to configure BackboneFast to improve convergence time if a link were to fail. Where should you configure the BackboneFast?
A: Switch CK4 only.
B: Switch CK2 and switch CK3 only.
C: Switch CK2 , switch CK3 and switch CK4 only.
D: Switch CK1 , switch CK2 , switch CK3 , and switch CK4 .

Answer: D

Explanation:
Backbone fast is a Cisco proprietary feature that, once enabled on all switches of a bridge network, can save a switch up to 20 seconds (max_age) when recovering from an indirect link failure.
You must enable BackboneFast on all switches in the network.
Note: The BackboneFast feature provides fast convergence in the network backbone after a spanning tree topology change occurs.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK6 21/technologies_tech_note09186a00800c2548.shtml

---

QUESTION 282:

What command would you enter, if you wanted to enable the spanning tree feature that causes a port to immediately switch from blocking to forwarding mode? (Type in answer below)

Answer: portfast

Explanation:
If you are connecting a workstation or a server with a single NIC card to a switch port, this connection cannot create a physical loop. These connections are considered leaf nodes. There is no reason to make the workstation wait 30 seconds while the switch checks for loops when the workstation cannot cause a loop. Cisco added the PortFast or fast-start feature, which means the STP for this port will assume that the port is not part

of a loop and will immediately move to the forwarding state, without going through the blocking, listening, or learning states. This command does not turn STP off. This command makes STP skip a few (unnecessary in this circumstance) steps in the beginning on the selected port.
The portfast variable, when enabled on a port, causes the port to immediately switch from blocking mode to forwarding mode. This helps prevent time-outs on clients that use Novell Netware or that use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address. However, it is important that you do not use this command when you have switch-to-switch connection. It could potentially result in a loop. The 30-60 second delay that occurs when transitioning from blocking to forwarding mode transition prevents a temporal loop condition in the network when connecting two switches.

QUESTION 283:

Which of the following are FALSE, when configuring load sharing by using STP path costs? (Select all that apply)

A. All priorities must be set to 100
B. Load-sharing links can connect to different switches
C. All priorities must be set to 0
D. The switch must be restarted for the second time
E. Both load-sharing links must connect to the same switch

Answer: A, C, D, E

Explanation:
The only true statement in the choices above is choice B. Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, Spanning-Tree Protocol (STP) normally blocks all but one parallel link between switches. With load sharing, you divide the traffic between the links according to which VLAN the traffic belongs to. There are two ways to configure load sharing by using trunk ports: using STP port priorities or using STP path costs. If you configure load sharing using STP port priorities, both load-sharing links must be connected to the same switch. If you configure load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

QUESTION 284:

CORRECT TEXT
If a switch is configured as a secondary root, what is the new default spanning tree bridge priority value? (Type in the answer below)

Answer: 16384

Explanation:
When you configure a switch as the secondary root, the spanning tree bridge priority is

modified from the default value (32768) to 16384. This means that the switch is likely to become the root bridge for the specified VLANs if the primary root bridge fails (assuming the other switches in the network use the default bridge priority of 32768).

QUESTION 285:

PortFast is being configured on switch CK1 . What should you take into consideration when configuring a switch with PortFast? (Select two choices below that are true statements)

A. It increases the forward delay time interval to 30 seconds.
B. It should be enabled on ports connecting to hubs and routers.
C. It should not be enabled on ports with redundant links to another switch.
D. It enables fast connectivity to be established on the access layer port to a booting workstation.

Answer: C, D

Explanation:
C: Portfast on redundant links could cause network loops when improperly used.
D: PortFast is used to make a point-to-point port almost immediately enter into forwarding state by decreasing the time of the listening and learning states.
Incorrect Answers:
A: PortFast decreases the forward delay time.
B: Ideally PortFast should only be used on point-to-point links connected only to workstations or servers.

QUESTION 286:

What should you take into consideration when configuring a switch with UplinkFast? (Select two.)

A. It must be used with the PortFast feature enabled.
B. When enabled, it is enabled for the entire switch and all VLANs.
C. It should be configured on all switches, including the root bridge.
D. When the primary Root Port uplink fails, another blocked uplink can be immediately brought up for use.

Answer: B, D

Explanation:
B: All VLANs on the switch are affected and you cannot configure UplinkFast on individual VLANs.
D: When a link fault occurs on the primary root link, UplinkFast transitions the blocked port to a forwarding state. UplinkFast changes the port without passing through the listening and learning phases.

Incorrect Answers:
A: These two features can be used independently from each other.
C: This is true of the Backbone fast, not of the uplink fast feature.

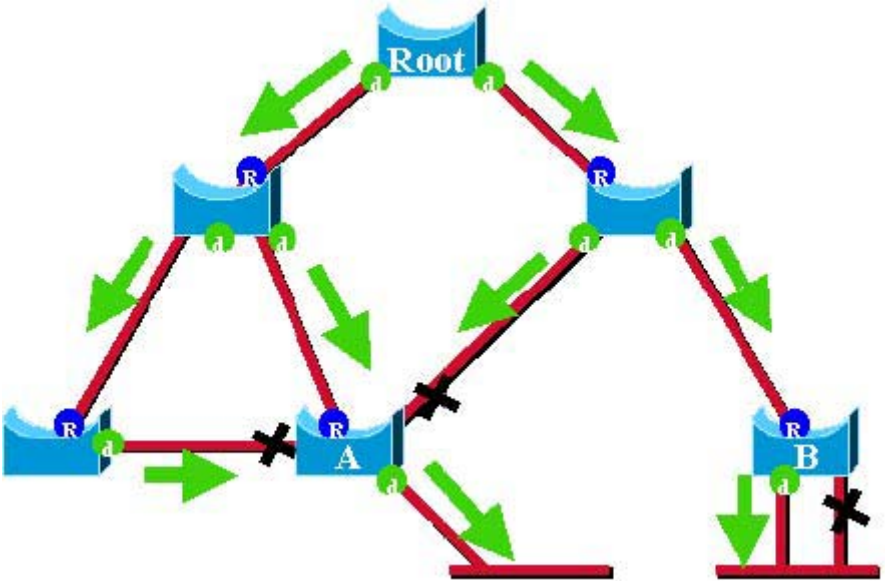
QUESTION 287:

Which three conditions need to be present for UplinkFast to trigger a fast reconfiguration? Choose three.

A. The switch must have at least one unblocked port.
B. The switch must have UplinkFast enabled.
C. The switch must be configured for one VLAN.
D. The switch must have at least one blocked port.
E. The failure must be on the root port.
F. The switch must be enabled on a VLAN with switch priority configured.

Answer: B, D, E

Explanation:
Uplink Fast Theory of Operation:
The UplinkFast feature is based on the definition of an uplink group. On a given switch, the uplink group consists in the root port and all the ports that provide an alternate connection to the root bridge. If the root port is failing (that is, if the primary uplink fails), a port with next lowest cost from the uplink group is selected to immediately replace it.
The following diagram helps to explain what the UplinkFast feature is based on:

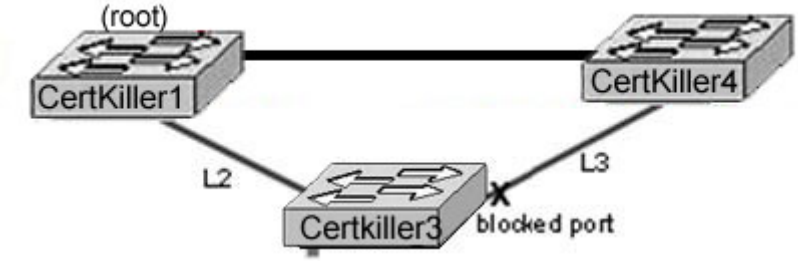


In this diagram, root ports are represented with a blue R and designated ports are represented with a green d. The green arrows represent the BPDUs generated by the root bridge and retransmitted by the bridges on their designated ports. Without entering a formal demonstration, we can determine the following about BPDUs and ports in a stable network:

1. When a port is receiving a BPDU, it has a path to the root bridge. This is because BPDUs are originated from the root bridge. In this diagram, check switch A: three of its ports are receiving BPDUs, and three of its ports lead to the root bridge. The port on A that is sending BPDU is designated and not leading to the root bridge.
2. On any given bridge, all ports receiving BPDUs are blocking, except the root port. A port receiving a BPDU is leading to the root bridge. If we had a bridge with two ports leading to the root bridge, we would have a bridging loop.
3.
A self-looped port does not provide an alternate path to the root bridge. See switch B in the diagram. Switch B's blocked port is self-looped, which means that it cannot receive its own BPDUs. In this case, the blocked port is not providing an alternate path to the root.
On a given bridge, the root port and all blocked ports that are not self-looped form the uplink group. The following section describes step-by-step how UplinkFast achieves fast convergence using an alternate port from this uplink group.
Note:UplinkFast is only working when the switch has blocked ports. The feature is typically designed for an access switch having redundant blocked uplinks. When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

QUESTION 288:

Three Certkiller switches are connected together as shown in the diagram below:

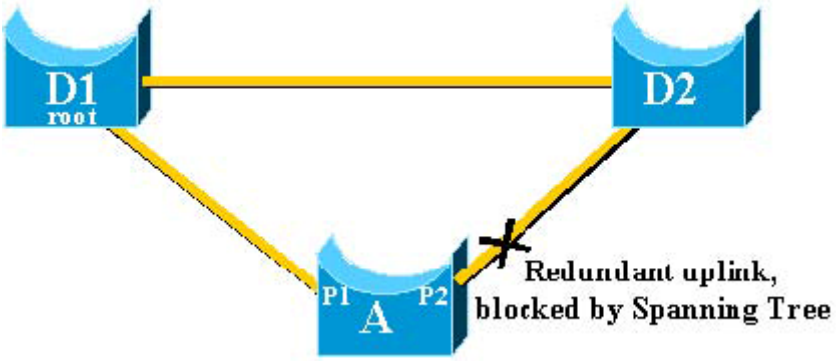


Switch Certkiller 1, the root bridge, is connected directly to Switch Certkiller 2 over Link L1 and to Switch Certkiller 3 over link L2. The Layer 2 LAN interface on Certkiller 3 that is connected directly to Certkiller 2 is in the blocking state. If Certkiller 3 detects a link failure on the currently active link L2 on the root port, which spanning tree enhancement will allow Switch Certkiller 3 to unblock the blocked port and transition it to forwarding without going through the listening and learning states?

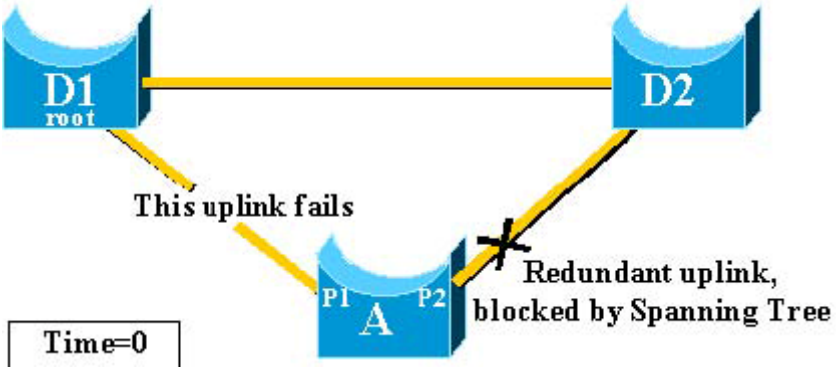
A. PortFast
B. UplinkFast
C. BackboneFast
D. Rapid spanning tree
E. None of the above

Answer: B

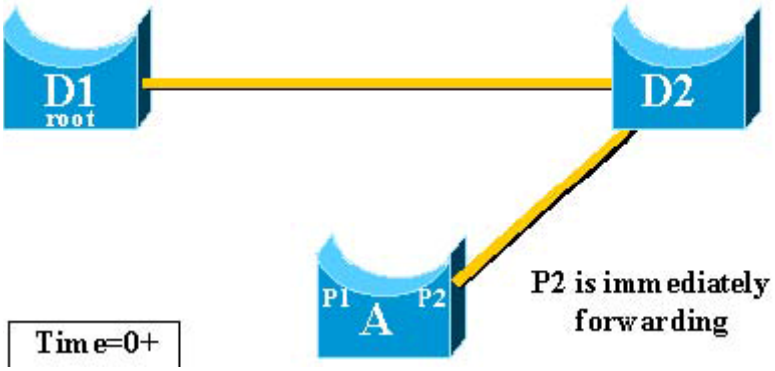
Explanation:
The following example explains the Uplink fast procedure step by step:
Uplink Failure WithUplink Fast Enabled
This section details the steps for UplinkFast recovery. We will use the network diagram that was introduced at the beginning of the document.
Immediate Switch Over to the Alternate Uplink



Follow these steps for an immediate switch over to the alternate uplink:
1. A's uplink group consists of P1 and its nonself-looped blocked port, P2.
2. When the link between D1 and A fails, A detects a link down on port P1.
It knows immediately that its unique path to the root bridge is lost (other paths are via the uplink group, for example, port P2 , which is blocked).



3. A places port P2 in forwarding mode immediately, thus violating the standard STP procedures.
We know that there will be no loop in the network, as the only path to the root bridge is currently down. Therefore, recovery is almost immediate.



Reference: http://www.cisco.com/warp/public/473/51.html

QUESTION 289:

Which statement is true about the STP Path Cost on a particular port?

A. It is known only to the local switch where the port resides.
B. It can be modified to help determine Root Bridge selection.
C. Modifying it can cause TCN BPDU to be sent to the Root Bridge.
D. When increased, it can provide higher bandwidth to a connecting port.
E. None of the above
F. All of the above.

Answer: A

Explanation:
When two ports on a switch are part of a loop, the spanning tree port priority and port path cost setting determine which port is put in the forwarding state and which port is put in the blocking state. The spanning tree port priority value represents the location of an interface in the network topology and how well located it is to pass traffic. The spanning tree port path cost value represents media speed.
The path cost is known locally to the switch only, as the pat cost information is not advertised to other switches within a network.
Incorrect Answers:
B: Modifying the cost may help determine which port is a root port, but it will not aid in the selection of the root switch since the path cost value is only known locally.
C: The cost information is only stored locally on the switch, so changes made are not propagated to other switches.
D: Although the cost is a direct reflection of the speed on an interface, it does not affect the actual bandwidth or throughput of an interface.

QUESTION 290:

Switch CK1 has been configured with the root guard feature. What statement is true if the spanning tree enhancement Root Guard is enabled?

A. If BPDUs are not received on a non-designated port, the port is moved into the STP loop-inconsistent blocked state
B. IF BPDUs are received on a PortFast enabled port, the port is disabled.
C. If superior BPDUs are received on a designated port, the interface is placed into the root-inconsistent blocked state.
D. If inferior BPDUs are received on a root port, all blocked ports become alternate paths to the root bride.

Answer: C

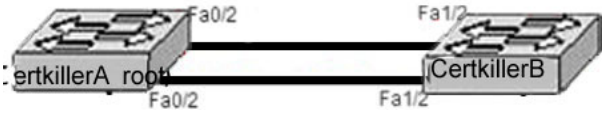
Explanation:

Root guard is configured on a per-port basis, and does not allow the port to become a STP root port. This means that the port is always STP-designated. If there is a better BPDU received on this port, root guard will put the port into root-inconsistent STP state, rather than taking the BPDU into account and electing a new STP root. Root guard needs to be enabled on all ports where the root bridge should not appear. In a way one can configure a perimeter around part of network where STP root is allowed to be located.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK6 21/technologies_tech_note09186a00800ae96b.shtml

---

QUESTION 291:

Exhibit



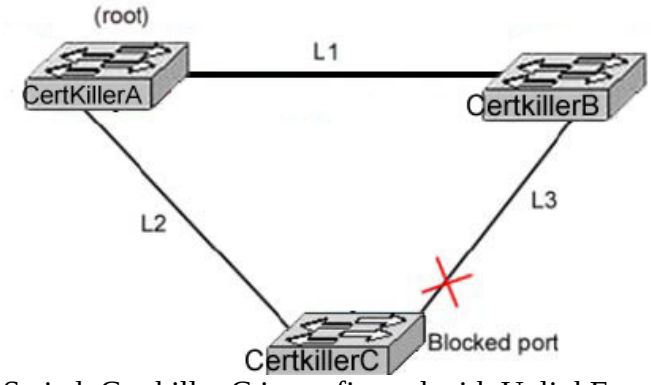
VLAN 1 and VLAN 2 are configured between the switches Certkiller A and Certkiller B in the exhibit.
What should be done to load balance VLAN traffic between Certkiller A and Certkiller B?

A. Lower the port priority for VLAN 1 on port 0/1 for Switch Certkiller A.
B. Lower the port priority for VLAN 1 on port 0/2 for Switch Certkiller A.
C. Make the bridge ID of Switch Certkiller B lower than Switch Certkiller A.
D. Enable ports 0/1 and 0/2 on Switch Certkiller A and 1/1 and 1/2 on Switch Certkiller B to be trunk ports.
E. Enable HSRP on the access ports.

Answer: A

QUESTION 292:

Exhibit, Network Topology



Switch Certkiller C is configured with UplinkFast. How much time will expire after a failure in L2 before Switch Certkiller C activates the port connected to L3?

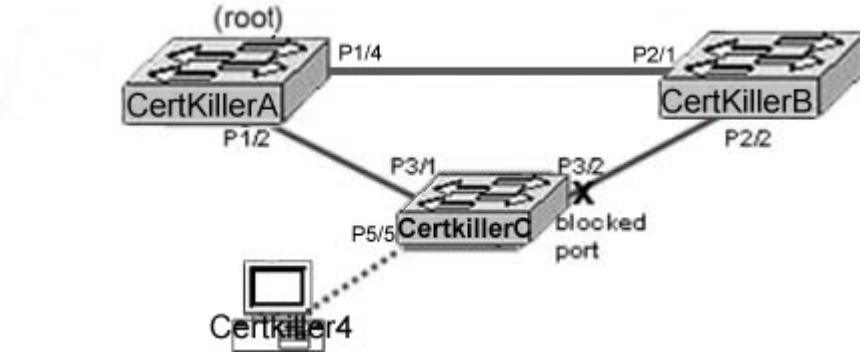
A. 1-5 seconds

B. 15 seconds
C. 30 seconds
D. 50 seconds

Answer: A

QUESTION 293:

Exhibit



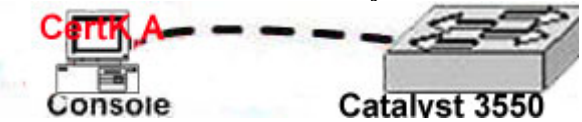
You work as a technician at Certkiller .com. Study the exhibit carefully. Spanning tree is enabled on all devices. Currently either Switch Certkiller B or Certkiller C can serve as the root should switch Certkiller A fail. A client recently connected to Device Certkiller 4, a PC running Windows XP SP2 and switching application software, to Switch Certkiller C port P3/3. You must configure Root Guard to ensure that the Certkiller 4 PC does not assume the role of the root. All other parameters must stay the same. On which interface(s) must Root Guard be enabled?

A. P1/2
B. P2/2
C. P3/3
D. P1/1 and P1/2
E. P1/2 and P2/2
F. P1/2, P2/2 and P3/3

Answer: C

QUESTION 294:

SIMULATION
You are connected to a Catalyst switch via a console cable as shown below:



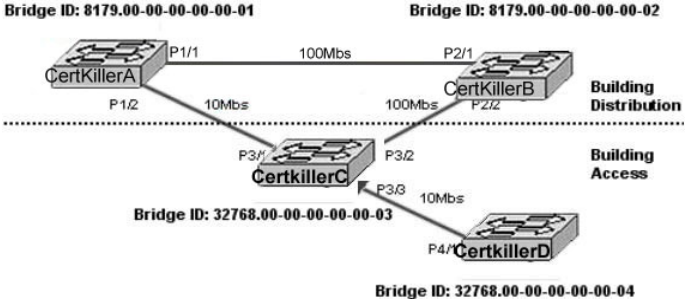
You work as a systems administrator at the Certkiller .com main office in the greater Toronto area. The number of employees on your floor has exceeded the infrastructure of your current network equipment. Your CTO has ordered a new switch chassis, but it's going to be another 6-8 working days until it arrives. In the

meantime you can to connect 24 new workstations to an old Cisco Catalyst 3550, which your junior administrator has just finished erasing, and rebooting (to purge old VLAN information).
Your tasks are to:
* disable VTP
* Ensure that all non-trunking interfaces do not participate in Spanning Tree by default by globally configuring PortFast.
For the following two tasks, you are required to use global commands to configure the ports:
1. Ensure all FastEthernet interfaces are in permanent non-trunking mode.
2. Place FastEthernet interfaces 0/12 through 0/24 in VLAN 20.
Start by clicking on host CertK iA.

Answer:
!
Switch(config)#show run (to check if vlan 20 exists already)
switch#vlan database (On the Switch 3550, the command (config)#vlan 20 not supported.)
switch(vlan)#vlan 20
switch(vlan)#exit
!
switch#configure terminal
switch(config)#vtp mode transparent (disable vtp)
switch(config)#interface range fa0/1 - 24 (select interfaces)
switch (config-if-range)#spanning-tree portfast ("Ensure that all FASTETHERNET interfaces")
switch(config-if-range)#switchport mode access (set ports for access mode, NOT Trunking)
switch(config-if-range)#exit
!
switch(config)#interface range fa0/12 - 24 (select interfaces)
switch(config-if-range)#switchport access vlan 20 (assign ports to vlan 20)
switch(config-if-range)#end
switch#copy running-config startup-config(save configuration)

QUESTION 295:

Exhibit



Based on the assumption that STP is enabled on all the switch devices, which of the following statements are true? (Choose two)

A. Certkiller A will be elected the root bridge.
B. Certkiller B will be elected the root bridge.
C. Certkiller C will be elected the root bridge.
D. P3/1 will be elected the nondesignated port.
E. P2/2 will be elected the nondesignated port.
F. P3/2 will be elected the nondesignated port.

Answer: A, D

QUESTION 296:

CORRECT TEXT
What command would you enter if you wanted to enable 'IP accounting' on one of your interfaces? (Type in answer below):

Answer: ip accounting

Explanation:
To enable IP accounting on an interface, use the ip accounting interface configuration command. To disable IP accounting, use the no form of this command.
ip accounting [access-violations]
no ip accounting [access-violations]

QUESTION 297:

VLANs are being implemented on the Certkiller network. What does Cisco recommend as the ideal ratio of VLANs to IP subnets?

A. One-to-one
B. Many-to-one
C. One-to-many
D. VLANs are mapped to MAC addresses
E. None of the above

Answer: A

Explanation:
Cisco Systems recommend a one-to-one correspondence between VLANs and IP subnets.
There should be a separate IP subnet for each VLAN.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 90.

QUESTION 298:

Which command could you use on a Catalyst 3550 switch if you wanted to set a port to operate as a nontrunking, single VLAN, Layer 2 interface so it will send and receives non-encapsulated (non-tagged) frames?

A. switchport
B. switchport mode access
C. switchport nonegotiate
D. switchport access vlan dynamic
E. None of the above

Answer: B

Explanation:
To set up a single vlan non trunking port you'll need to create a static VLAN membership. "The switchport mode access command configures the port for static VLAN membership."
Reference: CCNP Switching Exam Certification Guide: page 104, David Hucaby & Tim Boyles, Cisco Press 2001, ISBN 1-58720 000-7

QUESTION 299:

While logged into a Certkiller switch you issue the following command:
Certkiller Switch(config-mst)# instance 10 vlan 11-12
What does this command accomplish?

A. It enables a PVST+ instance of 10 for vlan 11 and vlan 12
B. It enables vlan 11 and vlan 12 to be part of the MST region 10
C. It maps vlan 11 and vlan 12 to the MST instance of 10.
D. It creates an Internal Spanning Tree (IST) instance of 10 for vlan 11 and vlan 12
E. It create a Common Spanning Tree (CST) instance of 10 for vlan 11 and vlan 12
F.
It starts two instances of MST, one instance for vlan 11 and another instance for vlan 12.

Answer: C

Explanation:
MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than Per VLAN Spanning Tree Plus (PVST+) and is backward compatible with 802.1D STP, 802.1w (Rapid Spanning Tree Protocol [RSTP]), and the Cisco PVST+ architecture.
MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other

instances.
Map the VLANs to an MST instance.
If you do not specify the vlan keyword, you can use the no keyword to unmap all the VLANs that were mapped to an MST instance.
If you specify the vlan keyword, you can use the no keyword to unmap a specified VLAN from an MST instance.
Switch(config-mst)# instance instance_number vlan vlan_range
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_guide_chapter09186a00800dd

---

QUESTION 300:

What happens when you apply an outgoing access list to an interface of a Catalyst switch?

A. it will purge any entries for flows on that interface and records no new entries
B. it will generate excessive MLSP messages
C. it will record packets only if the administrator sets the MLS RP IP ACL command on the interface
D. it will result in no action taken

Answer: A

Explanation:
According to Cisco; Traditionally, switches operated at Layer 2 only; switches switched traffic within a VLAN and routers routed traffic between VLANs. Catalyst 6000 family switches with the Multilayer Switch Feature Card (MSFC) can accelerate packet routing between VLANs by using Layer 3 switching (Multilayer Switching [MLS]). The switch first bridges the packet, the packet is then routed internally without going to the router, and then the packet is bridged again to send it to its destination. During this process, the switch can access control all packets it switches, including packets bridged within a VLAN. IOS ACLs access control routed traffic between VLANs, and VLAN ACLs (VACLs) access control all packets. Standard and extended IOS ACLs are used to classify packets. Classified packets can be subject to a number of features such as access control (security), encryption, policy-based routing, and so on. Standard and extended IOS ACLs are only configured on router interfaces and applied on routed packets.

QUESTION 301:

Some Cisco switches process Access Control Lists (ACL's) in their hardware. What would happen if the hardware reaches its maximum storage capacity of ACLs? (Select all that apply.)

A. Packets are dropped.
B. Packet filtering will be accomplished.

C. Performance is increased.
D. Performance is decreased.
E. None of the above

Answer: B, D

Explanation:
Determining if the ACL Configuration Fits in Hardware
As previously stated, ACL processing in the Catalyst 3550 switch is mostly accomplished in hardware. However, if the hardware reaches its capacity to store ACL configurations, the switch software attempts to fit a simpler configuration into the hardware. This simpler configuration does not do all the filtering that has been configured, but instead sends some or all packets to the CPU to be filtered by software. In this way, all configured filtering will be accomplished, but performance is greatly decreased when the filtering is done in software.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a008007e

---

QUESTION 302:

Switch CK1 is a Catalyst 3550. What kinds of access-control lists can you use on CK1 to filter traffic? (Select two)

A. CBAC
B. VLAN Maps
C. Router ACLs
D. Reflexive ACL

Answer: B, C

Explanation:
VLAN Maps and conventional access control lists are how the Catalyst 3550 switch filters traffic.
Incorrect Answers:
A, D: CBAC (Contact Based Access Control) and reflexive access lists are beyond the scope of this test, and are available on routers using specialized IOS versions.

QUESTION 303:

When authentication is required, where must 802.1x be configured in order to connect a PC to a switch?

A. client PC only
B. switch port only
C. switch port and client PC

D. switch port and RADIUS server

Answer: D

QUESTION 304:

Which process plays a major role in the creation of the CEF adjacency table? (811)

A. Address Resolution Protocol (ARP)
B. PDU header rewrite
C. NetFlow Switching
D. hello packet exchange

Answer: A

QUESTION 305:

In the use of 802.1X access control, which three products are allowed through the switch port before authentication takes place? Select three.

A. STP
B. CDP
C. EAP MD5
D. TACACS+
E. EAP-over-LAN
F. protocols not filtered by an ACL

Answer: A, B, E

QUESTION 306:

Which protocol does TACACS+ use to communicate between a TACACS+ server and a TACACS+ client?

A. UDP
B. TCP
C. IP
D. LEAP

Answer: B

QUESTION 307:

HSRP is being set up between two Certkiller devices. In what three states is it possible for an HSRP router to be in? (Select three)

A. Standby
B. Established
C. Active
D. Idle
E. Backup
F. Init

Answer: A, C, F

Explanation:
With HSRP, a set of routers work together to present the illusion of a single virtual router to the hosts on the LAN. This set is known as an HSRP group or a standby group. A single router elected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the Active router. Another router is elected as the Standby router. In the event that the Active router fails, the Standby assumes the packet-forwarding duties of the Active router. Although an arbitrary number of routers may run HSRP, only the Active router forwards the packets sent to the virtual router. Before a router becomes the active or standby router, it will be in the Init (initial) state.
Reference:
http://www.cisco.com/en/US/tech/ CK6 48/ CK3 62/technologies_tech_note09186a0080094a91.shtml

---

QUESTION 308:

What three tasks must a network administrator perform to properly configure Hot Standby Routing Protocol (HSRP)? (Select three)

A. Define the encapsulation type.
B. Define the standby router.
C. Define the standby IP address.
D. Enable the standby priority.

Answer: B, C, D

Explanation:
Three of the required configuration commands needed for enabling HSRP is to define the standby routing process, define the HSRP IP address, and configure the HSRP priority.
Configuring HSRP:
* Configuring an interface to participate in an HSRP standby group
* Assigning HSRP standby priority
* Configuring HSRP standby pre-empt
* Configuring HSRP over trunk links
* Configuring hello message timers
* HSRP interface tracking
* Displaying the status of HSRP
Incorrect Answers:

A: There are no encapsulation options for enabling HSRP.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 272

QUESTION 309:

To protect against first-hop router failure, four protocols were developed to ensure IP routing redundancy. Which of the following are they? (Select four)

A. HSRP
B. IRDP
C. ICMP
D. VRRP
E. MSTP
F. GLBP

Answer: A, B, D, F

Explanation:
A: HSRP is the Hot Standby Routing Protocol, which is the Cisco proprietary method for automatic failover and provides for redundant default gateways for hosts.
B: Some newer IP hosts use ICMP Router Discovery Protocol (IRDP) (RFC 1256) to find a new router when a route becomes unavailable. A host that runs IRDP listens for hello multicast messages from its configured router and uses an alternate router when it no longer receives those hello messages.
D: VRRP is the Virtual Router Redundancy Protocol, which is similar in many ways to HSRP. One key difference is that VRRP is standards based, where HSRP is Cisco developed.
F: Gateway Load Balancing Protocol (GLBP) protects data traffic from a failed router or circuit, like Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP), while allowing packet load sharing between a group of redundant routers.

QUESTION 310:

HSRP is compatible over which of the following networks? (Select all that apply)

A. Banyan VINES
B. IP
C. IBM DLC
D. Novell IPX
E. AppleTalk

Answer: A, B, D, E

Explanation:
According to the online documentation provided by Cisco:

You can configure HSRP in networks that, in addition to IP, run AppleTalk, Banyan VINES, and Novell IPX. AppleTalk and Novell IPX continue to function when the standby router becomes the active router, but they take time to adapt to topology changes. In general, AppleTalk hosts discover a new active router in less than 30 seconds. Novell 4.x hosts discover a new active router in 10 seconds, on average. Novell 2.x or Novell 3.x hosts might require more time to adapt.

QUESTION 311:

HSRP has been configured between two Certkiller devices. What kind of message does an HSRP configured router send out every 3 seconds? (Select all that apply)

A. Retire
B. Coup
C. Resign
D. Send
E. Hello

Answer: E

Explanation:
Hello-The hello message conveys to other HSRP routers the router's HSRP priority and state information. By default, an HSRP router sends hello messages every three seconds.
Incorrect Answers:
A, D: These messages are not used by HSRP.
B: Coup-When a standby router assumes the function of the active router, it sends a coup message. This message is used by HSRP, but it is not sent our every 3 seconds.
C: Resign-A router that is the active router sends this message when it is about to shut down or when a router that has a higher priority sends a hello message. This message is only sent before it resigns, not every 3 seconds.

QUESTION 312:

HSRP has been configured between two Certkiller devices. Which of the following describe reasons for deploying HSRP? (Select all that apply)

A. HSRP provides redundancy and fault tolerance
B. HSRP allows one router to automatically assume the function of the second router if the second router fails
C. HSRP allows one router to automatically assume the function of the second router if the second router starts
D. HSRP provides redundancy and load balancing

Answer: A, B, D

Explanation:

One way to achieve near-100 percent network uptime is to use HSRP, which provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits. By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single "virtual" router. The members of the virtual router group continually exchange status messages. This way, one router can assume the routing responsibility of another, should it go out of commission for either planned or unplanned reasons. Hosts continue to forward IP packets to a consistent IP and MAC address, and the changeover of devices doing the routing is transparent.
Through the use of multiple HSRP standby groups, traffic can be load balanced between the HSRP routers. For example, users on one VLAN could use one router as the primary HSRP router, and users on another VLAN can use the other HSRP router as the primary.

QUESTION 313:

Which one of the statements below correctly describes the Virtual Router Redundancy Protocol (VRRP)?

A. A VRRP group has one active and one or more standby virtual routers.
B. A VRRP group has one master and one or more backup virtual routers.
C. A VRRP group has one active and one or more standby virtual routers.
D. A VRRP group has one master and one redundant virtual router.

Answer: B

Explanation:
The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.
In a topology where multiple virtual routers are configured on a router interface, the interface can act as a master for one virtual router and as a backup for one or more virtual routers.
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1612/products_feature_guide09186a0080080a60.html

---

QUESTION 314:

You want to allow Router CK1 to immediately become the active router if its priority is highest than the active router fails. What command would you use if you wanted to configure this?

A. en standby preempt
B. standby preempt enable
C. standby preempt
D. hot standby preempt

Answer: C

Explanation:
The HSRP preemption feature enables the router with highest priority to immediately become the Active router. Priority is determined first by the priority value that you configure, and then by the IP address. In each case a higher value is of greater priority. When a higher priority router preempts a lower priority router, it sends a coup message. When a lower priority active router receives a coup message or hello message from a higher priority active router, it changes to the speak state and sends a resign message. To configure preemption, use the "standby standby-number preempt" command.

QUESTION 315:

Routers CK1 and CK2 are configured for HSRP as shown below:
Router CK1 :
interface ethernet 0
ip address 20.6.2.1 255.255.255.0
standby 35 ip 20.6.2.21
standby 35 priority 100
interface ethernet 1
ip address 20.6.1.1.2 255.255.255.0
standby 34 ip 20.6.1.21
Router CK2 :
interface ethernet 0
ip address 20.6.2.2 255.255.255.0
standby 35 ip 20.6.2.21
interface ethernet 1
ip address 20.6.1.1.1 255.255.255.0
standby 34 ip 20.6.1.21
standby 34 priority 100
You have configured the routers CK1 & CK2 with HSRP. While debugging router CK2 you notice very frequent HSRP group state transitions. What is the most likely cause of this?

A. physical layer issues
B. no spanning tree loops
C. use of non-default HSRP timers
D. failure to set the command standby 35 preempt

Answer: A

Explanation: CK2 is not able to from the standby state to reach the active state. This could be caused by missing HSRP hello messages. There are several possible causes for HSRP packets to get lost between the peers. The most common problems are Physical Layer Problems or excessive network traffic caused by Spanning-Tree

Issues.
Note:
Hot Standby Routing Protocol (HSRP) is a Cisco proprietary protocol used for allowing redundant connections. It can keep core connectivity if the primary routing process fails. HSRP defines six states in which an HSRP router may run: initial, learn, listen, speak, standby, and active.
Incorrect Answers:
B: Spanning tree loops does not affect this problem.
C: Not a likely cause. Besides, in the example here the default values were indeed used.
D: If the Preempt option is set, then an election of the Active router will take place. This process is called a coup. However, an election would take place by default.
Reference:
Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks
http://www.cisco.com/warp/public/473/62.shtml
RFC 2281, Cisco Hot Standby Router Protocol (HSRP)

QUESTION 316:

Which type of scheme describes the default operation of Gateway Load Balancing Protocol (GLBP)?

A. per host using a round robin scheme
B. per host using a strict priority scheme
C. per session using a round robin scheme
D. per session using a strict priority scheme
E. per GLBP group using a round robin scheme
F. per GLBP group using a strict priority scheme

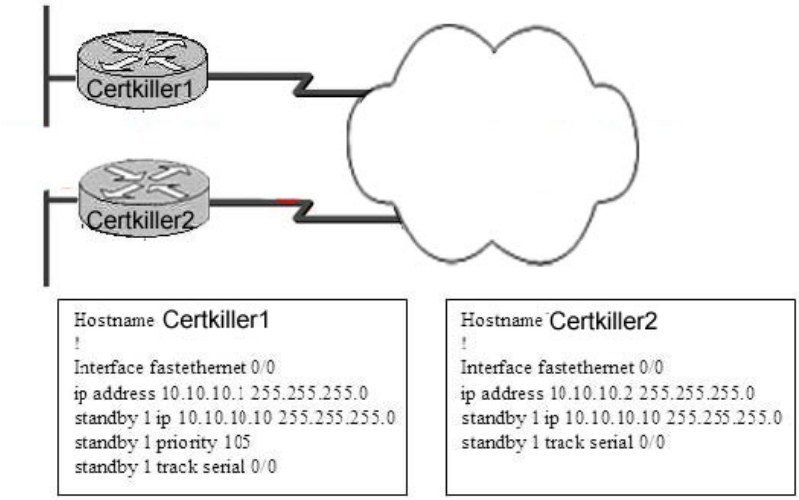
Answer: A

Explanation:
The Gateway Load Balancing Protocol feature provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first hop routers on the LAN combine to offer a single virtual first hop IP router while sharing the IP packet forwarding load. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.
GLBP performs a similar, but not identical, function for the user as the HSRP and the VRRP. HSRP and VRRP protocols allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, the hosts must be configured for different default gateways, which results in an extra administrative burden. GLBP provides load balancing over multiple routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers

in the virtual router group participate in forwarding packets. In this way, per host load balancing is achieved using a round robin mechanism.

QUESTION 317:

The Certkiller network is using two routers with HSRP for their Internet access as shown below:



Which command will need to be added to Certkiller 2 to ensure that it will take over if serial 0/0 on Certkiller 1 fails?

A. standby 1 preempt
B. standby 1 track 10.10.10.1
C. standby 1 priority 130
D. standby 1 track fastethernet 0/0
E. None of the above

Answer: A

Explanation:
When this command is configured, the router is configured to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router. If the hsrp preempt command is not configured, the local router assumes control as the active router only if it receives information indicating that no router currently is in the active state (acting as the designated router).
In this example, Certkiller 1 was properly configured to lower its own HSRP priority when the serial 0 interface goes down. However, even if this happens, router Certkiller 2 will not become the active router unless it is configured to pre-empt, or take over, if it suddenly has a higher priority than Certkiller 1.

QUESTION 318:

On a 3550 EMI switch, which three types of interfaces can be used to configure

HSRP? (Select three)

A. Loopback interface
B. SVI interface
C. Routed port
D. Access port
E. EtherChannel port channel
F. BVI interface

Answer: B, C, E

Explanation:
This
Hot Standby Router Protocol (HSRP) provides routing redundancy for routing IP traffic without being dependent on the availability of any single router. To use this feature, you must have the enhanced multilayer software image installed on your switch. All Catalyst 3550 Gigabit Ethernet switches ship with the enhanced multilayer software image (EMI) installed. Catalyst 3550 Fast Ethernet switches can be shipped with either the standard multilayer software image (SMI) or EMI pre-installed. You can order the Enhanced Multilayer Software Image Upgrade kit to upgrade Catalyst 3550 Fast Ethernet switches from the SMI to the EMI.
Only routed interfaces that provide access to hosts can be configured for HSRP. These interfaces include: routed Ethernet, routed fast Ethernet, routed Gigabit Ethernet, SVI, and EtherChannel.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_chapter09186a00800c9

QUESTION 319:

Which protocol is an extension of ICMP that allows an IP host on the Certkiller network to find a new router when a router becomes unavailable, as defined by RFC 1256?

A. ICMP (IRDP)
B. SNMP
C. HSRP
D. VRRP
E. None of the above

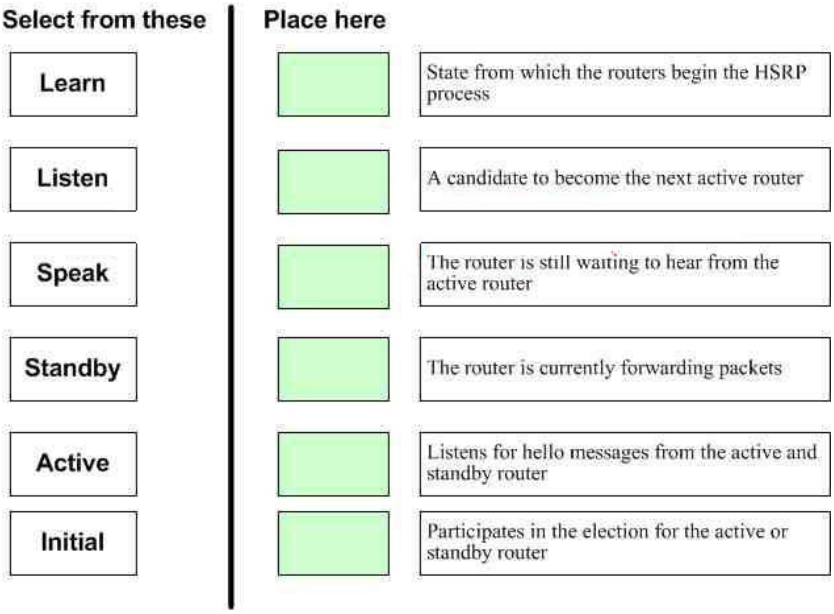
Answer: A

Explanation:
RFC 1256 defines the ICMP Router Discovery Protocol. Some newer IP hosts use ICMP Router Discovery Protocol (IRDP) to find a new router when a route becomes unavailable.

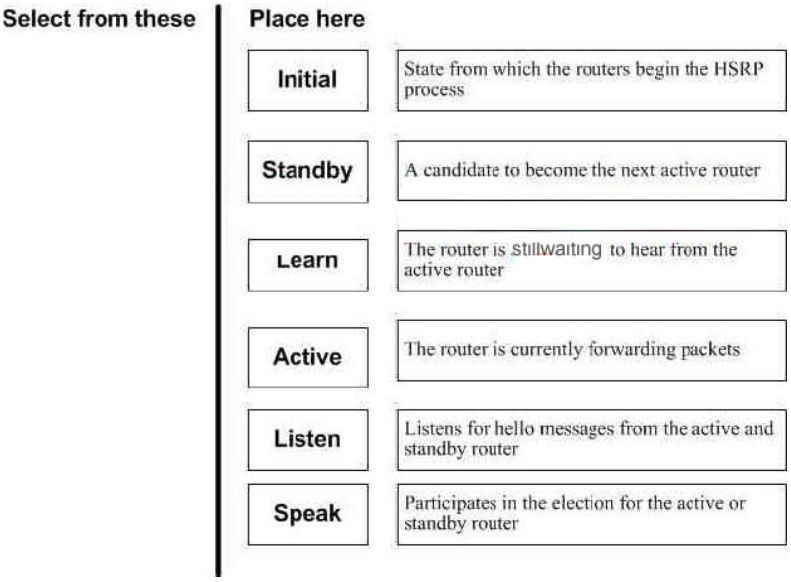
ICMP Router Discovery Protocol (IRDP) enables a host to determine the address of a router that it can use as a default gateway. Similar to ES-IS but used with IP.
Router discovery uses Internet Control Message Protocol (ICMP) router advertisements and router solicitation messages to allow a host to discover the addresses of operational routers on the subnet. Hosts must discover routers before they can send IP datagrams outside their subnet. Router discovery allows a host to discover the addresses of operational routers on the subnet.
Each router periodically multicasts a router advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts listen for advertisements to discover the addresses of their neighboring routers. When a host starts, it can send a multicast router solicitation to ask for immediate advertisements.
The router discovery messages do not constitute a routing protocol. They enable hosts to discover the existence of neighboring routers, but do not determine which router is best to reach a particular destination.
References: CCNP Switching Exam Certification Guide, David Hucaby CCIE #4594 & Tim Boyles. Cisco Press, ISBN 1-58720-000-7 Page 308 "IRDP is an extension to ICMP that provides a mechanism for routers to advertise useful default routes."
http://www.javvin.com/protocolIRDP.html
http://www.faqs.org/rfcs/rfc1256.html

QUESTION 320:

DRAG DROP
Match the HSRP states on the left with the correct definition on the right.



Answer:



QUESTION 321:

In the hardware address 0000.0c07.ac0av, what does 07.ac represent?

A. HSRP well-known physical MAC address
B. Vendor code
C. HSRP router number
D. HSRP group number
E. HSRP well-known virtual MAC address

Answer: E

Explanation:
HSRP code (HSRP well-known virtual MAC address) - The fact that the MAC address is for an HSRP virtual router is indicated in the next two bytes of the address. The HSRP code is always 07.ac. The HSRP protocol uses a virtual MAC address, which always contains the 07.ac numerical value.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 268

QUESTION 322:

The Certkiller network needs to enhance the reliability of the network. Which of the following protocols provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first-hop failures in network edge devices or access circuits, as defined by RFC 2281?

A. STP
B. IRDP
C. ICMP

D. HSRP

Answer: D

Explanation:
HSRP is defined in RFC 2281. The Hot Standby Router Protocol, HSRP, provides a mechanism which is designed to support non-disruptive failover of IP traffic in certain circumstances. In particular, the protocol protects against the failure of the first hop router when the source host cannot learn the IP address of the first hop router dynamically. The protocol is designed for use over multi-access, multicast or broadcast capable LANs (e.g., Ethernet). HSRP is not intended as a replacement for existing dynamic router discovery mechanisms and those protocols should be used instead whenever possible. A large class of legacy host implementations that do not support dynamic discovery are capable of configuring a default router. HSRP provides failover services to those hosts.
Reference: http://www.faqs.org/rfcs/rfc2281.html

QUESTION 323:

Which of the following protocols enables a group of routers to form a single virtual router, and then use the real IP address of a router as the gateway address, as defined in RFC 2338?

A. Proxy ARP
B. HSRP
C. IRDP
D. VRRP
E. GLBP

Answer: D

Explanation:
The Virtual Router Redundancy Protocol (VRRP) feature enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group. VRRP is defined in RFC 2338.
Reference: http://www.faqs.org/rfcs/rfc2338.html

QUESTION 324:

Routers can send hello messages in three HSRP states. Which ones are they? (Select three)

A. standby
B. learn
C. listen

D. speak
E. active

Answer: A, D, E

Explanation:
The various HSRP states are described below:
Listen: The router knows the virtual IP address, but is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak: The router sends periodic hello messages, and is actively participating in the election of the active and/or standby router. A router cannot enter speak state unless it has the virtual IP address.
Standby: The router is a candidate to become the next active router, and sends periodic hello messages. Excluding transient conditions, there would be at most one router in the group in standby state.
Active: The router is currently forwarding packets that are sent to the group's virtual MAC address. The router sends periodic hello messages. Excluding transient conditions, there must be at most one router in active state in the group.
Initial: This is the starting state, and indicates that HSRP is not running. This state is entered via a configuration change, or when an interface first comes up.
Learn: The router has not determined the virtual IP address, and has not yet seen an authenticated hello message from the active router. In this state, the router is still waiting to hear from the active router.

QUESTION 325:

Two Certkiller routers are configured for HSRP. Cisco's Hot Standby Routing Protocol (HSRP) can provide automatic router backup over which networks?

A. Ethernet and FDDI
B. Ethernet, FDDI and Token Ring LANs
C. Token Ring LANs only
D. VINES and IPX only
E. Ethernet and Token Ring LANs

Answer: B

Explanation:
Cisco's Hot Standby Routing Protocol (HSRP) provides automatic router backup when you configure it on Cisco routers that run the Internet Protocol (IP) over Ethernet, Fiber Distributed Date Interface (FDDI), and Token Ring local-area networks (LANs). HSRP is compatible with Novell's Internetwork Packet Exchange (IPX), AppleTalk, and Banyan VINES, and it is compatible with DECnet and Xerox Network Systems (XNS) in certain configurations.

QUESTION 326:

Exhibit

```
*Mar  1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar  1 00:16:43.099: SB:  VI11 Interface up
*Mar  1 00:16:43.099: SB11: VI11 Init: a/HSRP enabled
*Mar  1 00:16:43.099: SB11: VI11 Init -> Listen
*Mar  1 00:16:43.295: SB11: VI11 Hello  in  172.10.11.112 Active  prt 50 ip 172.10.11.115
*Mar  1 00:16:43.295: SB11: VI11 Active router is 1/2.16.11.112
*Mar  1 00:16:43.295: SB11: VI11 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar  1 00:16:43.295: SB11: VI11 Active router is local, was 172.16.11.112
*Mar  1 00:16:43.299: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Listen -> Active
*Mar  1 00:16:43.299: SB11: VI11 Hello  out 172.16.11.111 Active  pri 100 ip 172.16.11.115
*Mar  1 00:16:43.303: SB11: VI11 Hello  in  172.16.11.112 Speak  pri 50 ip 172.16.11.115
*Mar  1 00:16:46.207: SB11: VI11 Hello  out 172.16.11.111 Active  pri 100 ip 172.16.11.115
*Mar  1 00:16:49.095: SB11: VI11 Hello  in  172.16.11.112 Speak  pri 50 ip 172.16.11.115
```

Based on the debugoutput shown in the exhibit, which three statements about HSRP are true? Select three.

A. The final active router is 172.16.11.111
B. The 172.16.11.111 router has preempt configured.
C. The 172.16.11.112 router has a more preferred priority than the 172.16.11.111 router does.
D. 172.16.1.115 is the virtual HSRP IP address.
E. The 172.16.11.112 router has nonpreempt configured.
F. The 172.16.11.112 router is using default HSRP priority.

Answer: A, B, D

QUESTION 327:

Exhibit

```
CertKillerA# show standby
Ethernet0/1 group
  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 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
  IP redundancy name is "HSRP1", advertisement interval is 34 sec
```

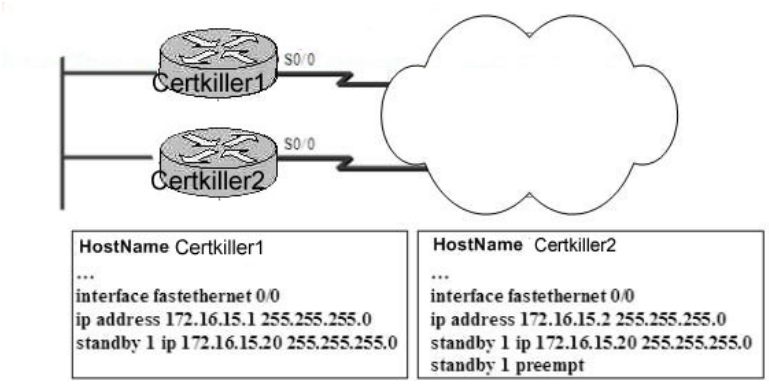
Study the router output displayed in the exhibit.
Which two items are correct? Select two.

A. Certkiller A will assume the active state if its priority is the highest.
B. If Ethernet 0/2 goes down, the standby router will take over.
C. When Ethernet 0/3 of Certkiller A comes back up, the priority will become 105.
D. The local IP address of Certkiller A is 10.1.0.6.
E. The local IP address of Certkiller A is 10.1.0.20.

Answer: A, C

QUESTION 328:

Exhibit



Which command will ensure that Certkiller 2 will be the primary router for traffic using the gateway address of 172.16.15.20?

A. On Certkiller 2 add the command standby 1 priority 80
B. On Certkiller 1 add the command standby 1 priority 110
C. On Certkiller 1 add the command standby 1 priority 80
D. On Certkiller 2 remove the command standby 1 preempt

Answer: C

QUESTION 329:

Which router redundancy protocol cannot be configured for interface tracking?

A. HSRP
B. GLBP
C. VRRP
D. SLB
E. RPR
F. RPR+

Answer: C

QUESTION 330:

What protocol specified by RFC 1256 will allow an enabled IP host a new router when a router becomes unavailable?

A. IRDP
B. SNMP

C. HSRP
D. VRRP

Answer: A

QUESTION 331:

Exhibit

```
*Mar  1 00:12:16.871: SB11: Vl11 Hello  in  172.16.11.112 Active  pri 50 ip 172.16.11.115
*Mar  1 00:12:16.871: SB11: Vl11 Active router is 172.16.11.112
*Mar  1 00:12:18.619: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar  1 00:12:18.623: SB:  Vl11 Interface up
*Mar  1 00:12:18.623: SB11: Vl11 Init: a/HSRP enabled
*Mar  1 00:12:18.623: SB11: Vl11 Init -> Listen
*Mar  1 00:12:19.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*Mar  1 00:12:19.819: SB11: Vl11 Hello  in  172.16.11.112 Active  pri 50 ip 172.16.11.115
*Mar  1 00:12:19.819: SB11: Vl11 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar  1 00:12:22.815: SB11: Vl11 Hello  in  172.16.11.112 Active  pri 50 ip 172.16.11.115
*Mar  1 00:12:22.815: SB11: Vl11 Listen: h/Hello rcvd from lower pri Active router
*Mar  1 00:12:25.683: SB11: Vl11 Hello  in  172.16.11.112 Active  pri 50 ip 172.16.11.115
*Mar  1 00:12:25.683: SB11: Vl11 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar  1 00:12:28.623: SB11: Vl11 Listen: d/ Standby times
*Mar  1 00:12:28.623: SB11: Vl11 Listen -> Speak
*Mar  1 00:12:28.623: SB11: Vl11 Hello  out 172.16.11.111 Speak  pri 100 ip 172.16.11.115
*Mar  1 00:12:28.659: SB11: Vl11 Hello  in  172.16.11.112 Active  pri 50 ip 172.16.11.115
*Mar  1 00:12:28.659: SB11: Vl11 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar  1 00:12:31.539: SB11: Vl11 Hello  in  172.16.11.112 Active  pri 50 ip 172.16.11.115
*Mar  1 00:12:31.539: SB11: Vl11 Speak: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar  1 00:12:31.575: SB11: Vl11 Hello  out 172.16.11.111 Speak  pri 100 ip 172.16.11.115
*Mar  1 00:12:34.491: SB11: Vl11 Hello  in  172.16.11.112 Active  pri 50 ip 172.16.11.115
```

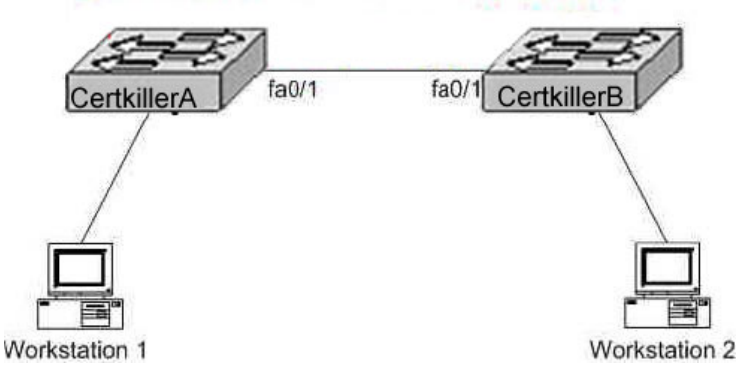
What can be determined about the HSRP relationship from the displayed debug output?

A. The pre-empt feature is not enable don the 172.16.11.111 router.
B. The nonpreempt feature is enabled on the 172.16.11.112 router.
C. Router 172.16.11.111 will be the activate router because its HSRP priority is preferred over router 172.16.11.112.
D. Router 172.16.11.111 will be the activate router because its HSRP priority is preferred over router 172.16.11.111.
E. The IP address 172.16.11.111 is the virtual HSRP router IP address.
F. The IP address 172.16.11.112 is the virtual HSRP router IP address.

Answer: A

QUESTION 332:

The Certkiller network is displayed in the following topology exhibit:



Workstation 1 traffic is set for cos 5 and the switch Certkiller A sends workstation 1 traffic to the switch Certkiller B. However, not all of the traffic from Switch Certkiller A is from workstation 1.
Switch Certkiller A configurations Switch Certkiller B Configuration:
mlsqos mls qos
interfacefa0/1 interface fa0/1
switchportmode trunk switchport trunk mode
switchporttrunk encapsulation dot 1q switchport trunk encapsulation dot 1q
switchporttrunk native vlan 1 switchport trunk native vlan 1
Frames from Workstation 1 are given the rightful priority through Switch Certkiller A, but Switch Certkiller B doesn't reciprocate, and treats Workstation 1 frames as if they have no precedence. Which of the following actions will prioritize traffic from Workstation 1?

A. Configure qos all command under Switch Certkiller B fa0/1 interface.
B. Configure mls qos trust cos command under Switch Certkiller B fa0/1 interface.
C. Configure mls qos trust cos 5 command under Switch Certkiller B fa0/1 interface.
D. Configure qos cos 5 command under Switch Certkiller B fa0/1 interface.
E. Configure mls qos trust cos command under Switch Certkiller A fa0/1 interface.
F. Configure qos cos 5 command under Switch Certkiller A fa0/1 interface.

Answer: B

Explanation:
The default action is for a switch with QoS features activated not to trust edge devices and any frames that enter the switch have their CoS re-written to the lowest priority of zero. If the edge device can be trusted, this default behaviour must be overridden and the access switch must be configured to switch the frame, leaving the CoS bits untouched.
The trust is configured on the switch port using the command:
switch(config-if)#mls qos trust cos

QUESTION 333:

You are a CCNP at Certkiller , and your incompetent junior administrator has incorrectly changed the MTU (maximum transmission unit) settings of the IP packets sent on an interface. What command would you enter if you wanted to restore the MTU size to its default? (Type in answer below)

Answer: no ip mtu

Explanation:
To set the maximum transmission unit (MTU) size of IP packets sent on an interface, use the ip mtu interface configuration command. To restore the default MTU size, use the no form of this command.
ip mtu bytes
no ip mtu

QUESTION 334:

Switch CK1 is an IOS-based switch. Which command could an administrator use to establish a traffic policy on this IOS based switch?

A. traffic-list
B. route-map
C. policy-map
D. policy-list
E. None of the above

Answer: C

Explanation:
The policy-map command is used to create a traffic policy. The purpose of a traffic policy is to configure the QoS features that should be associated with the traffic that has been classified in a user-specified traffic class or classes. A traffic policy contains three elements: a name, a traffic class (specified with the class command), and the QoS policies (which are detailed in the "Configuring the Modular Quality of Service Command-Line Interface" chapter of this book). The name of a traffic policy is specified in the policy-map CLI (for example, issuing the policy-map class1 command would create a traffic policy named class1).
Reference:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800b

QUESTION 335:

Which command would you enter if you had a Cisco 3550 switch, and you wanted to configure priority queuing on your gig0/1 interface?

A. Under the global configuration, configure "priority-queue out"
B. Under the global configuration, configure "interface priority-queue gig0/1"
C. Under the interface gig0/1, configure "priority-queue out"
D. Priority queuing is on by default

Answer: C

Explanation:
To configure priority queuing on an interface, use the "priority-queue" command in interface mode.
Incorrect Answers:
A, B: Assigning the queuing type is an interface configuration command and needs to be done in interface mode, not in the global configuration mode.
D: On interfaces faster than a T1, the default queuing method is first in, first out (FIFO).

QUESTION 336:

Switch CK1 and CK2 are connected via an ethernet channel as shown below:

Switch CK1:

```
interface port channel 1
switchport
switchport access vlan 10
interface fastethernet 0/1
channel-group 1 mode passive
interface fastethernet 0/2
channel-group 1 mode passive
```

Switch CK2

```
interface port-channel 1
switchport
switchport access vlan 10
interface fastethernet 0/1
channel-group 1 mode passive
interface fastethernet 0/2
channel-group 1 mode passive
```

In accordance with the above configuration, which of the statements below is correct?

A. PAgP is correctly configured and the EtherChannel will form.
B. LACP is correctly configured and the EtherChannel will form.
C. One switch must be in LACP Active mode for the EtherChannel to form.
D.
Only one switch must be in the On mode and the other in the LACP Passive mode for Etherchannel to form.
E. Each physical port in the EtherChannel must have the command switchport access vlan 10 for the EtherChannel to form.

Answer: C

Explanation:
Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer. It performs a similar function as Port Aggregation Protocol (PAgP) with Cisco EtherChannel.
To start automatic EtherChannel configuration with LACP, configure at least one end of the link to active mode to initiate channelling, because ports in passive mode passively respond to initiation and never initiate the sending of LACP packets.

QUESTION 337:

What does an EtherChannel port do if a VLAN range doesn't match its port list?

A. The ports will form EtherChannel if they are set to auto mode.
B. The ports will form EtherChannel if they are all set to the same trunk type.
C. The ports will not form an EtherChannel.
D. The ports will form an EtherChannel if the mode is set to on.

Answer: C

Explanation:
An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking EtherChannel. If the allowed range of VLANs is not the same for a port list, the ports do not form an EtherChannel even when set to the auto or desirable mode with the set port channel command.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800eb

---

QUESTION 338:

Which command would you enter on your Catalyst 2900XL switch if you wanted to enable an EtherChannel bundle?

A. Port group
B. Set port channel on
C. Port etherchannel enable
D. Set etherchannel port enable

Answer: A
Explanation
Under the interface command you have to indicate the syntax as port group (group number) for each interface you want to bundle in the etherchannel.
The port group command is used to enable an etherchannel bundle on a Catalyst 2900XL switch.
Incorrect Answers:
B: The set port channel command is not used on a Catalyst 2900XL switch. It used on other switches, such as Cisco 5000 series however.
C, D: These are invalid configuration commands.

QUESTION 339:

You have a Catalyst 5000 and you've just configured an Etherchannel bundle. If one of the links were to fail, how long will it take for traffic to be rerouted to a new link?

A. one minute
B. a few seconds
C. a few milliseconds
D. not until appropriate commands are entered

Answer: C

Explanation:

If a link is lost in an EtherChannel network, traffic is rerouted to one of the other links in just a few milliseconds. This rerouting is automatic, and the time it takes for traffic to get re-routed is normally not noticeable by end users.

QUESTION 340:

You are configuring a switching solution and you want to take advantage of the Fast EtherChannel ports. When configuring FastEthernet ports, which precautions can you take to avoid configuration problems which can cause the ports to be automatically disabled? (Select two)

A. Allow some ports in a channel to be partly disabled.
B. Configure ALL the ports in a channel as dynamic.
C. Assign all ports in a channel to the same VLAN
D. Allow some ports in a channel to be disabled.
E. Allow all ports in a channel to be disabled.
F. Configure all ports in a channel to operate at the same speed but in different duplex modes
G. Assign all ports in a channel to the same VLAN or configure them as trunk ports.

Answer: C, G

Explanation:
Cisco's Fast EtherChannel technology builds upon standards based 802.3 full duplex Fast Ethernet to provide network managers a reliable high speed solution for the campus network backbone. Fast EtherChannel provides bandwidth scalability within the campus by providing increments from 200 Mbps to 800 Mbps with multi-gigabit capacity in the future. Fast EtherChannel technology not only solves the immediate problem of scaling bandwidth within the network backbone today, but also paves the path for an evolution to standards-based Gigabit Ethernet and beyond, because Fast EtherChannel technology can be applied to support Gigabit EtherChannel.
In order for a channel to function properly, the aggregated links should be in the same VLAN or the links should be assigned as a trunk. In addition, all links should have identical speed and duplex settings.

QUESTION 341:

You have just configured an EtherChannel bundle on switch CK1 and it is now operational on a trunk. Which of the following could cause the disabling of the ports in this bundle? (Select two)

A. Disabling port security
B. Excessive errors on one port
C. Changing the VLAN mode to dynamic
D. Changing the speed attribute of one port in the bundle.

Answer: C, D

Explanation:
C: Do not configure the ports in an EtherChannel as dynamic VLAN ports. It could adversely affect switch performance.
D: All ports in an EtherChannel should be configured to operate at the same speed and duplex mode (full or half duplex).
Reference: Cisco, Configuring Fast EtherChannel and Gigabit EtherChannel

---

QUESTION 342:

Switch CK1 is a Catalyst 5000 switch. Which of the following set commands would you use to enable Fast EtherChannel on this switch?

A. "set channel fast"
B. "set port channel"
C. "set link channel"
D. "set etherchannel"
E. None of the above

Answer: B

Explanation:
In order to configure ports on a switch to belong to an etherchannel bundle, use the "set port channel" configuration command. For example: set port channel 3/1-2 will configure ports 3/1 and 3/2 to belong to the channel.
Reference: Cisco Application Note, Understanding and Designing Networks Using Fast EtherChannel Technology

---

QUESTION 343:

Cisco switches use a logical operation to determine which links to send EtherChannle traffic. What kind of logical operation is it?

A. OR
B. AND
C. XOR
D. NAND

Answer: C

Explanation:
EtherChannel performs the XOR operation, which works like this:
A B C
0 XOR 0 -> 0
0 XOR 1 -> 1

1 XOR 0 -> 1
1 XOR 1 -> 0

QUESTION 344:

Which of the following commands would you enter if you wanted to find out whether or not switch CK1 is capable of supporting EtherChannel?

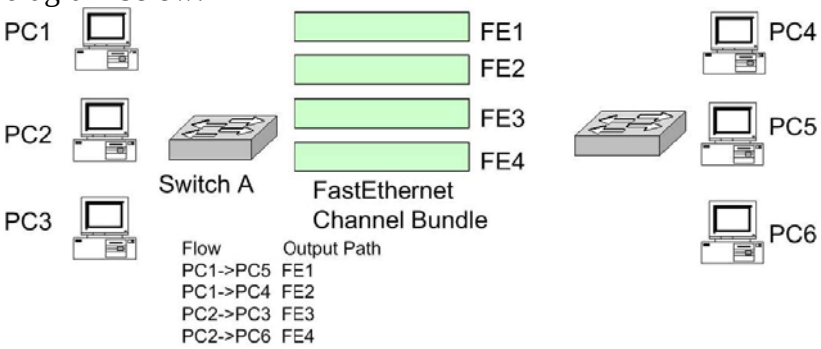
A. show trunk
B. show interface
C. show port channel
D. show port capabilities

Answer: D

Explanation:
The show port capabilities command will show you the capabilities of the modules and ports in a switch. For example, it will display the type, speed, and duplex.
Incorrect Answers:
A: Trunking information does not include the required information.
B: Interface configuration information does not include the required information.
C: Use the show port channel command to display EtherChannel information for a specific module or port. It will not show the capabilities of the switch of the switch however.

QUESTION 345:

Switch A and Switch B are configured for FastEthernet Channel as shown in the diagram below:



Assuming that Fast EtherChannel was set properly set up; if FEI were to fail, what would happen with the traffic flow between PC1 & PC5?

A. Traffic is transferred to FE2.
B. Traffic is transferred to FE4.
C. PC1 to PC4 traffic is distributed over the remaining links.
D. The session is disconnected while spanning tree rebuilds.

Answer: C

Explanation:
If a port within an EtherChannel fails, traffic previously carried over the failed port switches to the remaining ports within the EtherChannel.
Note: Fast/Gigabit EtherChannel allow high-speed redundant links in a spanning tree by allowing dual parallel links to be treated as though they were one link. If a link is lost in a Fast/Gigabit EtherChannel network, traffic rerouted to one of the other links in just a few milliseconds.
Reference: Configuring Fast EtherChannel and Gigabit EtherChannel
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/rel7_1/config/channel.htm

---

QUESTION 346:

You are configuring a switching solution and you want to take advantage of the Fast EtherChannel ports. When configuring FastEthernet ports, which precautions can you take to avoid configuration problems which can cause the ports to be automatically disabled? (Select two)

A. Allow some ports in a channel to be partly disabled.
B. Configure ALL the ports in a channel as dynamic.
C. Configure all ports in a channel to operate at the same speed and duplex mode
D. Assign all ports in a channel to the same VLAN or configure them as trunk ports.

Answer: C, D

Explanation:
Cisco's Fast EtherChannel technology builds upon standards based 802.3 full duplex Fast Ethernet to provide network managers a reliable high speed solution for the campus network backbone. Fast EtherChannel provides bandwidth scalability within the campus by providing increments from 200 Mbps to 800 Mbps with multi-gigabit capacity in the future. Fast EtherChannel technology not only solves the immediate problem of scaling bandwidth within the network backbone today, but also paves the path for an evolution to standards-based Gigabit Ethernet and beyond, because Fast EtherChannel technology can be applied to support Gigabit EtherChannel.
In order for a channel to function properly, the aggregated links should be in the same VLAN or the links should be assigned as a trunk. In addition, all links should have identical speed and duplex settings.

QUESTION 347:

Under what circumstances should an administrator prefer local VLANs over end-to-end VLANs?

A. Eighty percent of traffic on the network is destined for Internet sites.
B. There are common sets of traffic filtering requirements for workgroups located in

multiple buildings.
C. Eighty percent of a workgroup's traffic is to the workgroup's own local server.
D. Users are grouped into VLANs independent of physical location.
E. None of the above

Answer: A

Explanation:
This geographic location can be as large as an entire building or as small as a single switch inside a wiring closet. In a geographic VLAN structure, it is typical to find 80 percent of the traffic remote to the user (server farms and so on) and 20 percent of the traffic local to the user (local server, printers, and so on).
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 93

QUESTION 348:

What are some virtues of implementing end-to-end VLANs? (Choose two)

A. End-to-end VLANs are easy to manage.
B. Users are grouped into VLANs independent of a physical location.
C. Each VLAN has a common set of security and resource requirements for all members.
D. Resources are restricted to a single location.

Answer: B, C

Explanation:
In an end-to-end VLAN, users are grouped into VLANs independent of physical location and dependent on group or job function.
Each VLAN has a common set of security requirements for all members.
Incorrect Answers:
A: End to end VLANs are more difficult to manage than local VLANs, due to the physical distances that they can span.
D: In an end-to-end VLAN, network resources are generally distributed across the entire enterprise wide area network.

QUESTION 349:

Which of the following statements is true about the 80/20 rule (Select all that apply)?

A. 20 percent of the traffic on a network segment should be local
B. no more than 20 percent of the network traffic should be able to move across a backbone.
C. no more than 80 percent of the network traffic should be able to move across a backbone.
D. 80 percent of the traffic on a network segment should be local

Answer: B, D

Explanation:
The 80/20 rule in network design originated from Pareto's Principle. The Italian economist Vilfredo Paretto came up with the discovery that 20% of the people controlled 80% of the wealth and applied the principle of how inputs don't match outputs in real life. Keeping this number in mind, 80% of network traffic should be local to a segment and 20% should move across the backbone.
Note: With the availability of inexpensive bandwidth and centralized data centers, this rule appears to have become obsolete. In fact, most networks have taken on the 20/80 rules, as opposed to the legacy 80/20 rule.

QUESTION 350:

Which two factors give merit to the 20/80 LAN traffic model? (Select two)

A. The Internet
B. Local servers
C. Server farms
D. Localized applications
E. More powerful desktop PC's

Answer: A, C

Explanation:
Remote services (server farms, Internet, etc.) are factors which contributed to increased backbone traffic.
Also consider:
This geographic location can be as large as an entire building or as small as a single switch inside a wiring closet. In a geographic VLAN structure, it is typical to find 80 percent of the traffic remote to the user (server farms and so on) and 20 percent of the traffic local to the user (local server, printers, and so on).
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 93

QUESTION 351:

Which feature assigns switch ports to VLANs dynamically based on the source MAC address of the device connected to the port?

A. Dynamic VLAN Protocol
B. Dynamic Trunking Protocol
C. VLAN Database
D. VLAN Management Policy Server

Answer: D

Explanation
With VMPS (VLAN Management Policy Server), you can assign switch ports to VLANs dynamically, based on the source Media Access Control (MAC) address of the device connected to the port. When you move a host from a port on one switch in the network to a port on another switch in the network, the switch assigns the new port to the proper VLAN for that host dynamically.
When you enable VMPS, a MAC address-to-VLAN mapping database downloads from a Trivial File Transfer Protocol (TFTP) server and VMPS begins to accept client requests. If you reset or power cycle the switch, the VMPS database downloads from the TFTP server automatically and VMPS is re-enabled.
VMPS opens a User Datagram Protocol (UDP) socket to communicate and listen to client requests. When the VMPS server receives a valid request from a client, it searches its database for a MAC address-to-VLAN mapping.

QUESTION 352:

What method could you use to eliminate unicast and broadcast traffic that is flooded to a VLAN unnecessarily?

A. VTP pruning
B. MLS-SE
C. VTP trunking
D. VTP compression
E. All of the above

Answer: A

Explanation:
VTP ensures that all switches in the VTP domain are aware of all VLANs. There are occasions, however, when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded all over the VLAN. All switches in the network receive all broadcasts, even in situations where few users are connected in that VLAN. VTP pruning is a feature used to eliminate (prune) this unnecessary traffic.

QUESTION 353:

You are a network engineer and you've been assigned the task of configuring an Ethernet media trunk between two Cisco switches. Assuming that these two switches have the same modules, software revisions and VLAN configurations, which of the following are NOT true for the trunk to operate? (Choose all that apply)

A. The link must be a point to point for ISL encapsulation.
B. The link must be 100Mbs or slower
C. The link must use the IEEE 802.1Q trunk protocol.
D. The link may use the IEEE 802.1Q trunk protocol.

E. The link can operate at 10, 1000, or 100 Mbs interfaces

Answer: C, E

Explanation:
Trunks can operate at 10, 100, or 1000 Mbps interfaces.
The industry standard method of trunking is 802.1Q. As an alternative to this, the Cisco proprietary ISL method is also an option for setting up trunks.
Incorrect Answers:
A: This statement is true. ISL trunks must be configured on point to point links; point-to-multipoint configurations are not supported.
D: This statement is also true. 802.1Q can be used, but it does not have to be.

QUESTION 354:

Is the following statement True or False?
MLSP can cross a VTP domain boundary.

A. False
B. True
C. There is not enough information to determine

Answer: A

Explanation:
MLS requires that MLS components, including the end stations, must be in the same Virtual Trunking Protocol (VTP) domain. VTP is a Layer 2 protocol used for managing VLANs on several Catalyst switches from a central switch. It allows an administrator to create or delete a VLAN on all switches in a domain without having to do so on every switch in that domain. The MultiLayer Switching Protocol (MLSP), which the MLS-SE and the MLS-RP use to communicate with one another, does not cross a VTP domain boundary.

QUESTION 355:

The Certkiller LAN is becoming saturated with broadcasts and multicast traffic.
What could you do to help a network with many multicasts and broadcasts?

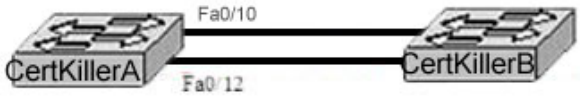
A. Creating smaller broadcast domains by implementing VLANs.
B. Separate nodes into different hubs.
C. Creating larger broadcast domains by implementing VLANs.
D. Separate nodes into different switches.
E. All of the above.

Answer: A

Explanation:
Controlling broadcast propagation throughout the network is important to reduce the amount of overhead associated with these frames. Routers, which operate at Layer 3 of the OSI model, provide broadcast domain segmentation for each interface. Switches can also provide broadcast domain segmentation using virtual LANs (VLANs). A VLAN is a group of switch ports, within a single or multiple switches, that is defined by the switch hardware and/or software as a single broadcast domain. A VLAN's goal is to group devices connected to a switch into logical broadcast domains to control the effect that broadcasts have on other connected devices. A VLAN can be characterized as a logical network.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 8

QUESTION 356:

Exhibit




```
Hostname CertkillerB
..
Interface fastethernet 0/10
spanningtree vlan 1-5 port priority 10
switchport mode trunk
!
Interface fastethernet 0/12
spanningtree vlan 6-10 port priority 10
switchport mode trunk
```

Refer to the exhibit. Which two statements are true about VLAN traffic? Select two.

A. VLANs 1-5 will be blocked if fa0/10 goes down.
B. VLANs 1-5 will use fa0/10 as a backup only.
C. VLANs 6-10 will use fa0/10 as a backup only.
D. VLANs 6-10 have a port priority of 128 on fa0/0.
E. VLANs 1-10 are configured to load share between fa0/10 and fa0/12.

Answer: C, E

QUESTION 357:

FIFO (First-In-First-Out) queue is associated with which QoS model?

A. Less than Best Effort Model
B. Best Effort Model
C. Differentiated Services Model (DiffServ)
D. Integrated Services Model (IntServ)
E. None of the above

Answer: B

Explanation:
There are three QoS Models namely, Integrated Services Model, Best effort Model, and Differentiated Services model.Best effort is a single service model in which an application sends data whenever it must, in any quantity, without requesting permission or first informing the network. For best-effort service, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. The Cisco IOS QoS feature that implements best-effort service is FIFO queuing.

QUESTION 358:

You are an instructor at Certkiller and one of your students has a few questions about QoS. After class she comes into your office, and asks, "If I wanted to configure congestion avoidance, what mechanism randomly drops packets with a certain IP precedence value when the buffers fill to a predefined threshold?" Which mechanism is she asking about?

A. WFQ
B. CQ
C. LLQ
D. WRED
E. tail drop

Answer: D

Explanation:
WRED drops packets using IP precedence or DSCP value of the packets; packets with higher precedence are less likely to be dropped. If the default settings are preventing QoS, the precedence value can be used to control how WRED determines when and how often to drop packets.

QUESTION 359:

WRED is being configured on different network devices throughout the Certkiller network. What is true about WRED?

A. Cisco Express Forwarding cannot be enabled with WRED.
B. WRED is useful when the bulk of traffic is not TCP/IP.
C. The rate of packet-drop decreases as the average queue size increases, until the average queue size reaches the maximum threshold.
D. Packets not flagged by IP precedence are randomly dropped when the average queue depth is above the minimum threshold.
E. WRED defines packet-drop probability using an access list.
F. All of the above.

Answer: D

Explanation:
Weighted Random Early Detection (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. This mechanism is used to avoid network congestion and give priority to certain traffic types.

QUESTION 360:

You are a CCNP working for a large online studio in Amsterdam. Your network team has redesigned its 'campus style' network in a way that it support three switch blocks, and these switch blocks act as broadcast domains to each individual switch block, while still allowing inter-VLAN routing within and between switch blocks. Which of the following switches is the best distribution layer device for your needs?

A. Catalyst 2900 series switch
B. Catalyst 3000 series switch
C. Catalyst 1900
D. Catalyst 4000 series switch
E. Catalyst 5000 series switch with l RSM
F. Catalyst 8500 series switch

Answer: E

Explanation:
Modules for the Catalyst 5000 family chassis --- Catalyst 5500, 5509, 5505, 5000, and 5002---are designed for complete interoperability and investment protection. New functionalities in the Catalyst 5000 family support multiprotocol NetFlow Switching for scalable convergence of Layer 2 and Layer 3 switching, adding the benefits of multiprotocol, multilayer switching and other Cisco IOS network services. The range of media support in the Catalyst 5000 family enables network managers to deliver high-performance backbone access to accommodate Web browser-based traffic across the intranet. A growing number of interface modules operate in any Catalyst 5000 family switch to deliver dedicated bandwidth to users through high-density group switched 10BaseT or 100BaseT Ethernet; flexible 10/100BASE-T Ethernet, fiber-based Fast Ethernet, and Fast EtherChannel; Token Ring; CDDI/FDDI; ATM LAN Emulation (LANE) and Multiprotocol over ATM (MPOA); the Router/Switch module (based on the Router/Switch processor for the Cisco 7500 series router); and
Gigabit Ethernet. Unique
to the Catalyst 5500 Series are the ATM Switch Processor and ATM switch interface modules and port adapters.

QUESTION 361:

What does a Catalyst 5000 switch need installed in order for MLS to run on it?
(Select all that apply)

A. IOS V13
B. IOS V12.11
C. Netflow Feature Card
D. The MLS-SE RP Card

Answer: C

Explanation:
The MLS-SE is a switch with special hardware. For a member of the Catalyst 5000 family, MLS requires that the supervisor have a Netflow Feature Card (NFFC) installed. The Supervisor IIG and IIIG have one by default. In addition, a bare minimum of Catalyst OS 4.1.1 software is also required. Note that the 4.x train is now in General Deployment (GD), or passed rigorous end-user criteria and field-experience targets for stability, so check Cisco's website for the latest releases. IP MLS is supported and automatically enabled for Catalyst 6000 hardware and software with the MSFC/PFC (other routers have MLS disabled by default). Note that IPX MLS and MLS for multicasting may have different hardware and software (Cisco IOS and Catalyst OS) requirements. More Cisco platforms do/will support the MLS feature. Also, MLS must be enabled in order for a switch to be an MLS-SE.

QUESTION 362:

A technical institute has redesigned its campus network to support three switch blocks of 2,000 users per block. The network administrator wants to control broadcast domains to each individual switch block, while still allowing interVLAN routing within and between switch blocks. What distribution layer device should be used to accomplish this?

A. Catalyst 4000 series switch
B. Catalyst 8500 series switch
C. Catalyst 6000 series switch with an internal MSFC
D. Catalyst 1900 with a two-port 100Base uplink module.

Answer: C

Explanation:
A Catalyst 6000 series switch with an internal MSFC (Multilayer Switch Feature Card) is the most appropriate solution. Catalyst 6000 series switches use the MSFC and the Policy Feature Card (PFC) to gather and cache header information.
Note:
Catalyst 6000 Family switches equipped with MSFCs provide transparent Web Cache redirection using Cisco's Web Cache Communication Protocol v2 (WCCP). WCCP is the

industry's leading web-cache redirection protocol that localizes network traffic and provides network- intelligent load distribution.

QUESTION 363:

Your CTO has authorized you to purchase 10 new switches that can support the VLAN Management Policy Server (VMPS) feature. Which three of the following switches can you consider? (Select three)

A. 2900XL series
B. 3500XL series
C. 5000 series
D. 8500 series

Answer: A, B, C

Explanation:
A, B: Catalyst 2900 and 3500 Series XL Features include VMPS.
C: VMPS functionality is present on all Catalyst 5000 Family switches.
Note: The VLAN Management Policy Server (VMPS) service is used to set up a database of MAC addresses that can be used for dynamic addressing of VLANs. VMPS is a MAC-address-to-VLAN mapping database.

QUESTION 364:

You are a salesman at a Cisco network equipment shop, when one of your regular customers, a CTO of a college comes in. He wants to launch a multimedia center to distribute her program information throughout the campus.
1. High availability
2. Gigabit data transfer speed
3. Access aggregation
4. InterVLAN routing between users and Server Farms
What should you recommend?

A. Catalyst 2948G-L3
B. Catalyst 4000 series switch
C. Catalyst 6000 series switch
D. Catalyst 7100 series switch

Answer: C

Explanation:
The Catalyst 6000 switches provide high-density Fast Ethernet and Gigabit Ethernet in both campus-backbone and server-aggregation environments. The Catalyst 6006 and the Catalyst 6009 switches have a 32-Gbps switching capacity, while the Catalyst 6506, the Catalyst 6509, the Catalyst 6509-NEB, and the Catalyst 6513 switches support a

backplane architecture that scales from 32 Gbps to 256 Gbps.
Incorrect Answers:
A: The Catalyst 2948G-L3 provides an aggregate throughput of 10 Mbps for Layer 3 switching. However, the requirement is of gigabit speed.
B: Not adequate.
D: Catalyst 7100 Series are VPN routers. Packet throughput is 175 Kpps. It is adequate for large branch and central site VPN router, for a dedicated site-to-site VPN solution.

QUESTION 365:

Which of the following switches utilize Cisco Express Forwarding (CEF)? (Select two)

A. Catalyst 8500
B. Catalyst 2900XL
C. Catalyst 3500XL
D. Catalyst 2948G-L3

Answer: A, D

Explanation:
A: Catalyst 8500 switches use a forwarding information base (FIB) for Cisco Express Forwarding.
D: The Catalyst 2948G-L3 uses Cisco Express Forwarding (CEF).
Note: Cisco Express
Forwarding (CEF) is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.
CEF was originally developed for the Cisco 12000 series gigabit switch router (GSR), the Catalyst 8500, and the Cisco 7500.
Incorrect Answers
B, C: These switches do not support CEF.
Reference: Cisco, Cisco Express Forwarding

QUESTION 366:

You are a salesman at an authorized Cisco dealer. A customer comes into your store asking for a switch that supports redundant supervisor engines. Which models would you show him? (Select all that apply)

A. Catalyst 4000
B. Catalyst 5500
C. Catalyst 6000
D. Catalyst 12000

Answer: B, C

Explanation:
B: The Catalyst 5500 series switches support an optional redundant supervisor engine.
C: Catalyst 6000 family switches support fault resistance by allowing a redundant supervisor engine to take over if the primary supervisor engine fails.

QUESTION 367:

Which of the following switches have an IOS-based user interface?

A. Catalyst 2924XL
B. Catalyst 2926
C. Catalyst 4003
D. Catalyst 5500

Answer: A

Explanation:
Catalyst 2924XL has an IOS-based user interface.
Note: Switches can either be IOS-based or set-based.
With IOS based user interface you can configure the switch from a CLI (command line interface) that is very similar to the ones used on Cisco routers. Catalyst 1900, 2820, and 2900 switches can be used with an IOS-based CLI.
Set-based user interface uses older, set-bases CLI configuration commands. The Cisco switches that use the set-based CLI are the 2926 series, the 1945G, the 4000, the 5000, and the 6000 series.

QUESTION 368:

You are a salesperson at an authorized Cisco dealership. A customer comes in wanting a switch, but reveals to you that he's IOS illiterate and only knows how to use the set-based CLI commands? Which models will you show him? (Select three)

A. 2900XL
B. 2948G
C. 3500XL
D. 4000
E. 6500

Answer: B, D, E

Explanation:
A 2948G, 4000, 5000, and 6500 series switch uses set based CLI commands.
Incorrect Answers:

2900XL and 3500XL switches do not use set based CLI commands. These switches are IOS based, and are configured similarly to a Cisco router.

QUESTION 369:

Your business venture is rapidly expanding and you need to provide access for numerous users and need a high density switch at the lowest possible price. Which of the following switches has the lowest price per port?

A. Catalyst 1900 series
B. Catalyst 3500XL series
C. Catalyst 5000 series
D. Catalyst 85000 series

Answer: C

Explanation:
A Catalyst 5000 series switch would be the optimal solution in this scenario. Although a 5000 series is not the cheapest switch that Cisco offers, it does have the lowest cost per port due to its high port density.

QUESTION 370:

A switched Ethernet costsconsiderably more to set up than a shared Ethernet using hubs. What justifies the added expense? (Select two.)

A. It provides greater scalability
B. It is less complex to manage
C. It permits full-duplex operation
D. It simplifies routing between LAN segments

Answer: A, C

Explanation:
A: A switched Ethernet has more collision domains, and each collision domain is smaller compared to Shared Ethernet. A switched Ethernet can therefore support more nodes compared to a shared Ethernet.
C: A switched connection may support full-duplex operation. Shared Ethernet is only half duplex.
Incorrect Answers:
B: A shared Ethernet requires less administration compared to a switched Ethernet.
D: Switches operates at Layer 2, the data link layer. Routing is performed at Layer 3, the network layer.

QUESTION 371:

The Certkiller LAN is using VLANs, and traffic between them needs to be routed. What kind of network equipment do you need for interVLAN routing?

A. ISL
B. switch block
C. IEEE 802.1Q
D. access switch
E. route processor

Answer: E

Explanation:
The traffic has to be routed between the VLANs. A routing mechanism has to be provided for interVLAN communication. This can either be accomplished using a router or a route processor within the switch.
Incorrect Answers:
A, C: Either IEEE 802.1Q or ISL trunking protocol can be used, but these are trunking protocols, not network hardware.
B, D: Neither of these is used for interVLAN routing.

QUESTION 372:

You're a salesperson at a network equipment wholesaler. A customer comes in and tells you that he needs a distribution layer switch for a large campus style network, with a high amount of Gigabit Ethernet port density. Which device series would you recommend to him?

A. 4908G-L3
B. 5000 series
C. 6000 series
D. 8500 series

Answer: C

Explanation:
The Catalyst 6000 can provide up to 384 10/100 Ethernet connections, 192 100FX FastEthernet connections, and 130 Gigabit Ethernet ports.
Incorrect Answers:
A, B: A 4908G-L3 switch or a Catalyst 5000 series switch are not capable of the required performance.
D: The Cisco Catalyst 8500 is a core layer switch that provides high-performance switching. This particular customer is looking for a distribution layer switch, not a core switch.

QUESTION 373:

Which of the following mechanisms combines the speed of switching with the scalability of routing?

A. Layer 3 switching
B. Fast switching
C. Layer 2 routing
D. Process routing
E. All of the above

Answer: A

Explanation:
Layer 3 switching is hardware-based routing. In particular, packet forwarding is handled by specialized hardware ASICs. A layer 3 switch does everything to a packet that a traditional router does.
Reference: Building Cisco Multilayer Switched Networks (Cisco Press) page 18

QUESTION 374:

Which three of the following network features are methods used to achieve high availability? (Select all that apply.)

A. Spanning Tree Protocol (STP)
B. Delay reduction
C. Hot Standby Routing Protocol (HSRP)
D. Dynamic routing protocols
E. Quality of Service (QoS)
F. Jitter management

Answer: A, C, D

Explanation:
Because the importance of high availability networks is increasingly being recognized, many organizations are beginning to make reliability/availability features a key selection criteria for network infrastructure products. With this in mind, Cisco Systems engaged ZD Tag to observe and confirm the results of a series of tests demonstrating the high availability features of Cisco Catalyst Layer 2/Layer 3 switches. In order to maximize the relevance of the results, the demonstration was based on a model of a "real world" campus (in one of Cisco's Enterprise Solution Center labs in San Jose, California). This switched internetwork consisted of wiring closet, wiring center, and backbone switches and conformed to Cisco's modular three-tier (Access/Distribution/Core) design philosophy. The testing demonstrated the following high availability and resilience features of Catalyst switches:
1. per-VLAN Spanning Tree (PVST) using Cisco's InterSwitch Link (ISL) and 802.1Q VLAN Trunking
2. Cisco Spanning Tree Enhancements, including UplinkFast and PortFast

3. Cisco Hot Standby Router Protocol (HSRP) and HSRP Track
4. Cisco IOS per-destination load balancing over equal cost OSPF paths
5. Cisco IOS fast convergence for OSPF
Reference:
http://www.cisco.com/warp/public/779/largeent/learn/technologies/campuslan.pdf

---

QUESTION 375:

You are a network administrator of a large investor relations company that uses a switched network to carry both data and IP telephony services. Why should you carry voice traffic on a separate VLAN?

A. IP phones require inline power and must be in separate VLAN to receive inline power.
B. IP telephony applications require prioritization over other traffic as they are more delay sensitive.
C. IP phones can only receive IP addresses through DHCP if they are in separate VLAN.
D. The CDP frames from the IP phone can only be recognized by the switch if the phone is in an auxiliary vlan.

Answer: B

Explanation:
Voice conversations don't take up a lot of bandwidth, but the bandwidth they do is very delicate. If anything happens with the connection or the integrity of the data transfer in either direction the conversation won't seam natural. To ensure the highest degree of integrity you should put voice traffic on its own separate VLAN and give that VLAN the highest priority.

QUESTION 376:

Which of the following switches have inline power support for Cisco IP telephony? (Select three)

A. 3500 series
B. 4000 series
C. 5000 series
D. 6000 series

Answer: A, B, D

Explanation:
A: With the expansion of inline power needs for IP phones and wireless access points, the Catalyst 3524-PWR XL is the leading choice.
B: The Cisco Catalyst 4000 Family Inline Power 10/100BaseT Ethernet Switching Module intelligently detects and provides power to IP enabled devices such as Cisco IP Phones.

D: The Cisco Catalyst 6000 Family Inline Power 10/100BaseT Ethernet Switching Module extends the voice capabilities of the Catalyst backbone to the enterprise wiring closet and branch office.
Note 1: Each Cisco IP Telephone provides Toll-quality audio and doesn't require a companion PC. Because it is an IP-based telephone, it can be installed anywhere on a corporate local or wide area IP network.
Note 2: Inline power is 48-volt DC power provided over standard Category 5 unshielded twisted-pair (UTP) cable up to 100 meters. Instead of requiring wall power, terminal devices such as IP telephones can utilize power provided from the Catalyst Inline Power Patch Panel.
Incorrect Answers:
C: Catalyst 5000 series switches are used in large campuses to provide access for more than 250 users. They support 10/100/1000Mbps Ethernet switching. They don't support inline power for Cisco IP phones, however.

QUESTION 377:

You're a network administer and you issue the command (show port 3/1) on an Ethernet port. To your surprise you notice a non-zero entry in the 'Giants' column. What could be the cause of this?

A. IEEE 802.1Q
B. IEEE 802.10
C. Misconfigured NIC
D. User configuration
E. All of the above

Answer: A
The 802.1Q standard can create an interesting scenario on the network. Recalling that the maximum size for an Ethernet frame as specified by IEEE 802.3 is 1518 bytes, this means that if a maximum-sized Ethernet frame gets tagged, the frame size will be 1522 bytes, a number that violates the IEEE 802.3 standard. To resolve this issue, the 802.3 committee created a subgroup called 802.3ac to extend the maximum Ethernet size to 1522 bytes.
Note: The show port command is used to display port status and counters. Giants denote the number of received giant frames (frames that exceed the maximum IEEE 802.3 frame size) on the port.
Reference: Trunking between Catalyst 4000, 5000, and 6000 Family Switches Using 802.1q Encapsulation
http://www.cisco.com/warp/public/473/27.html

QUESTION 378:

You have a trunk link operating between two switches and you're experiencing problems with frames leaking between the two VLANs. Each switch has identical modules, software revisions and VLAN configuration information. Spanning tree

protocol is disabled on all VLANs. What is probably causing this problem? (Select all that apply)?

A. The link is using IEEE 802.1Q protocol
B. The link is using IEEE 802.1E protocol
C. Spanning tree is disabled
D. Not enough information to determine.
E. The native VLAN information is identical at each end of the link.
F. The native VLAN information is different at each end of the link.

Answer: A, F

Explanation:
While internal to a switch, VLAN numbers and identification are carried in a special extended format that allows the forwarding path to maintain VLAN isolation from end to end without any loss of information. Instead, outside of a switch, the tagging rules are dictated by standards such as ISL or 802.1Q.
ISL is a Cisco proprietary technology and is in a sense a compact form of the extended packet header used inside the device: since every packet always gets a tag, there is no risk of identity loss and therefore of security weaknesses.
On the other hand, the IEEE committee that defined 802.1Q decided that because of backward compatibility it was desirable to support the so-called native VLAN, that is to say, a VLAN that is not associated explicitly to any tag on an 802.1Q link. This VLAN is implicitly used for all the untagged traffic received on an 802.1Q capable port.
This capability is desirable because it allows 802.1Q capable ports to talk to old 802.3 ports directly by sending and receiving untagged traffic. However, in all other cases, it may be very detrimental because packets associated with the native VLAN lose their tags, for example, their identity enforcement, as well as their Class of Service (802.1p bits) when transmitted over an 802.1Q link.
For these sole reasons-loss of means of identification and loss of classification-the use of the native VLAN should be avoided.
Reference:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

---

QUESTION 379:

What command could you enter to display the trunking status of a module/port in the switch? (Type in the answer below):

Answer: show trunk

Explanation:
Use the show trunk command to display trunking information for the switch.
show trunk [mod_num[/port_num]] [detail]mod_num (Optional) Number of the module.
/port_num (Optional) Number of the port.
detail (Optional) Keyword to show detailed information about the specified trunk port.

QUESTION 380:

You are troubleshooting a Catalyst 5000 trunk in the Certkiller network. What should you do if there's a disagreement about the VLANs configured to use the trunk?

A. Reload the active VLAN configuration
B. Clear the affected port and bring it up again.
C. Explicitly set the trunk for the VLAN to be on.
D. Remove all the VLANs set

Answer: B

Explanation:
In this situation you may want to set or clear the VLANS on both ends. A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network. Two trunking encapsulations are available on all Ethernet interfaces:
Inter-Switch Link (ISL)-ISL is a Cisco-proprietary trunking encapsulation
802.1Q-802.1Q is an industry-standard trunking encapsulation
When a trunk is first brought up using either of these methods, it may be beneficial to clear the port immediately after.

QUESTION 381:

You want to check your Catalyst switch port to see if there's an active link state. Which of the following actions would NOT be useful? (Select all that apply)

A. Switch fan
B. Port's link LED of the Switching Module.
C. Switch RP
D. Switch slot
E. Switch backplane

Answer: A, C, D, E

Explanation:
To find out if there is an active link state on a Catalyst port, check the port's link LED. As an alternative, using various show commands will also aid in troubleshooting port problems. However, checking the fan, RP, slot, or backplane will not help when looking for the status of an individual port's link status.

QUESTION 382:

Which of the following commands could you use to clear a switch of its current configuration?

A. the "clear config all" command
B. the "del config all" command
C. the "erase config all" command
D. the "clean config all" command
E. None of the above

Answer: A

Explanation:
In a Cisco switch, the 'clear config all' command will purge the existing configuration on a switch and start you off with a brand new default configuration. All the other commands; del, erase and clean; aren't valid IOS commands.

QUESTION 383:

Which kind of management can be performed from the console port of a Cisco 6500 switch?

A. Physical management of the switch.
B. Logical management of the switch.
C. In-band management of the switch.
D. Out-of-band management of the switch.

Answer: D

Explanation:
When you configure a switch or a router from the console, it is considered 'out of band' because you don't get in there from any of the paths that the network device is a part of. Modems are often attached to the console port, providing for remote out of band management of the device.

QUESTION 384:

A VTP domain named Certkiller has six active VLANs. Without notice, all VLANs except VLAN1 fail. Just prior to the failure, Switch Certkiller 2 was added to the network.
Which three issues on Switch Certkiller 2 could be the cause? Select three.

A. Switch Certkiller 2 is configured for only VLAN1.
B. Switch Certkiller 2 is a VTP server in a different domain.
C. Switch Certkiller 2 is a VTP server in the Certkiller domain.
D. Switch Certkiller 2 is not a VTP domain.
E. Switch Certkiller 2 has a lower VTP configuration revision number than the current

VTP revision.
F. Switch Certkiller 2 has a higher VTP configuration revision number than the current VTP revision.

Answer: A, C, F

Explanation: A VTP server in a given domain with the highest revision number will overwrite the VTP configuration of all other switch in the same VTP domain. Cisco best practices advises one to configure the correct VTP domain, VTP password, VTP mode, (server, client, transparent), and VTP revision number before adding any new switch to a network. The default VTP mode is server. A network can have more than one VTP domain. Each VTP domain has it own server(s) that do not influence clients in other VTP domains.

QUESTION 385:

You work as a network Technician at Certkiller .com. A new workstation has consistently been unable to obtain an IP address from the DHCP server when the workstation boots. Older workstations function normally, and the new workstation obtains an address when manually forced to renew its address.
What should be configured on the switch to allow the workstation to obtain an IP address at boot?

A. UplinkFast on the switch port connected to the server
B. BackboneFast on the switch port connected to the server
C. PortFast on the switch port connected to the workstation
D. trunking on the switch

Answer: C

QUESTION 386:

What should you do to reduce spanning-tree protocol BPDU traffic during extended periods of instability in your VLANs?

A. Combine all the VLAN spanning trees into a single spanning tree.
B. Set forward delay and max-age timers to the maximum possible values.
C. None of the choices.
D. Change the router VTP server mode.
E. Disable the root bridge

Answer: B

Explanation:
There are several STP timers, as listed below:
1. hello: the hello time is the time between each Bridge Protocol Data Unit (BPDU) that

is sent on a port. This is equal to two seconds by default, but can be tuned to be between one and ten seconds.
2. forwarddelay: the forward delay is the time spent in the listening and learning state. This is by default equal to 15 seconds, but can be tuned to be between four and 30 seconds.
3. maxage: the max age timer controls the maximum length of time a bridge port saves its configuration BPDU information. This is 20 seconds by default and can be tuned to be between six and 40 seconds.
The STP timers (hello, forward delay, and max age) are included in each BPDU. An IEEE bridge is not concerned about its local configuration of the timers value. It will consider the value of the timers contained in the BPDU that it is receiving. Effectively, that means only a timer configured on the root bridge of the STP is important. Obviously, in case you would lose the root, the new root would start to impose its local timer value to the entire network. So, even if it is not required to configure the same timer value in the entire network, it is at least mandatory to configure any timer changes on the root bridge and on the backup root bridge.
In order to reduce the number of BPDU's in the spanning tree topology, the forward delay and max-age timers should be increased. This will reduce the BPDU traffic, but it will also increase the convergence time during a topology change.

QUESTION 387:

You are network consultant troubleshooting a problem at Certkiller Inc. The local technician tells you that users can't access the Domain Controllers or DHCP servers from their workstations. To top it off, they aren't seeing their Novel Login Screen and they can't access their AppleTalk network. The customer use Cisco 4000, Cisco 5000, and Cisco 6000 switches. What command could you use to resolve these problems?

A. spanning-tree portfast
B. set port connect mod/port
C. spantree start-forwarding
D. set spantree portfast mod/port enable

Answer: D

Explanation:
When the switch powers up, or when a device is connected to a port, the port normally enters the spanning tree listening state. When the forward delay timer expires, the port enters the learning state. When the forward delay timer expires a second time, the port is transitioned to the forwarding or blocking state. This delay could cause the problems described in the scenario. We remove the delay with the PortFast feature. We enable PortFast on a switch port connected to a single workstation or server with the set spantree portfast mod_num/port_num enable command.
Note: The spanning tree PortFast feature causes a port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states. You can use

PortFast on switch ports connected to a single workstation or server to allow those devices to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state.
Reference: Cisco, Configuring Spanning Tree PortFast, UplinkFast, and BackboneFast

---

QUESTION 388:

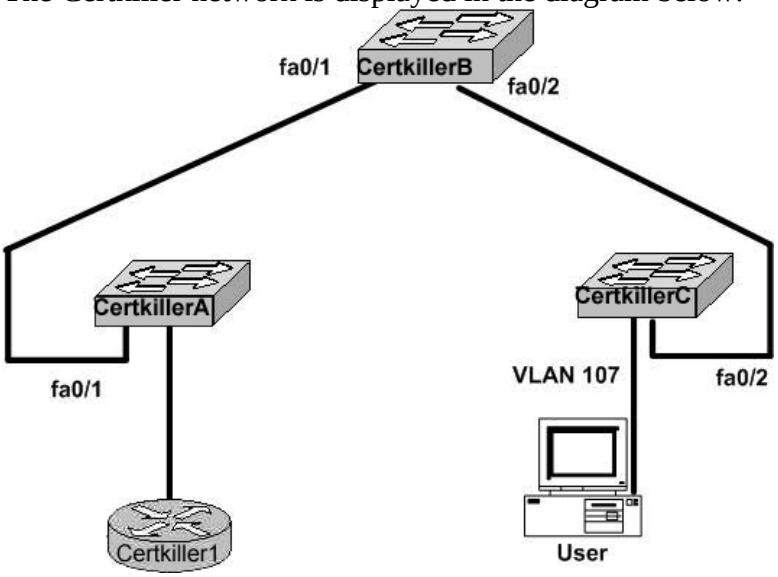
What command should you enter if do you want to find out whether or not the Backbone Fast convergence feature of STP is enabled on switch CK1 ? (Type in answer below):

Answer: show spantree backbonefast

Explanation:
The following list various commands to use for troubleshooting Catalyst switches:
show spantree vlan_id - Shows the current state of the spanning tree for the "vlan_id" entered from the perspective of the switch on which it is entered.
show spantree summary - Provides a summary of connected spanning tree ports by VLAN.
show spantree statistics - Shows spanning tree statistical information.
show spantree backbonefast - Displays whether the spanning tree Backbone Fast Convergence feature is enabled.
show spantree blockedports - Displays only the blocked ports.
show spantree portstate - Determines the current spanning tree state of a Token Ring port within a spanning tree.
show spantree portvlancost - Shows the path cost for the VLANs on a port.
show spantree uplinkfast - Shows the uplinkfast settings.

QUESTION 389:

The Certkiller network is displayed in the diagram below:



You use the following information for switch Certkiller A:
Port Mode Encapsulation Status Native VLAN
fa0/1 desirable n-802.1q trunking 5
Port VLANs is allowed on trunk
fa0/ 1 1-100, 102-1005
Port VLANs is owned and active in management domain
fa0/1 1-6. 8-100, 102-115, 197-999, 1002-1005
Port VLANs in spanning tree forwarding state and not pruned
fa0/1 1-6, 8-100, 102-105, 108-999, 1002-1005
Certkiller users in VLAN 107 complain that they are unable to gain access to the resources through the Certkiller 1 router.
What is the cause of this problem?

A. VLAN 107 is not configured on the trunk.
B. VLAN 107 does not exist on switch Certkiller A.
C. VTP is pruning VLAN 107.
D. Spanning tree is not enabled on VLAN 107.
E. None of the above

Answer: C

Explanation:
In this example, VLAN 7, 101, 106, and 107 are being pruned. VLAN 107 is being pruned incorrectly in this case. By disabling VTP pruning, VLAN 107 should be able to once again gain access to the network resources.
Incorrect Answers:
A, B: Based on the output shown above, VLAN 107 is known and active within the management domain. Therefore, it must have been configured and the VLAN is indeed allowed to traverse the trunk. Only VLAN 101 has been configured to not pass along this trunk.
D: By default, STP is enabled on all VLANs.

QUESTION 390:

Which of the following commands would you enter if you wanted to display spanning tree statistical information?

A. show spantree backbonefast
B. show spantree statistics
C. show spantree uplinkfast
D. show spantree blockedports
E. show spantree portstate
F. show spantree portvlancost

Answer: B

Explanation:
The command 'show spantree statistics' is the correct IOS command to show spanning tree statistical information and is obviously the correct answer choice.
The following list various commands to use for troubleshooting Catalyst switches:
show spantree vlan_id - Shows the current state of the spanning tree for the "vlan_id" entered from the perspective of the switch on which it is entered.
show spantree summary - Provides a summary of connected spanning tree ports by VLAN.
show spantree statistics - Shows spanning tree statistical information.
show spantree backbonefast - Displays whether the spanning tree Backbone Fast Convergence feature is enabled.
show spantree blockedports - Displays only the blocked ports.
show spantree portstate - Determines the current spanning tree state of a Token Ring port within a spanning tree.
show spantree portvlancost - Shows the path cost for the VLANs on a port.
show spantree uplinkfast - Shows the uplinkfast settings.

QUESTION 391:

Is the following statement True or False?
The "show spanning-tree" command only shows information about ports with their red or amber lights on.

A. True
B. There is not enough information to determine
C. False

Answer: C

Explanation:
The show spanning-tree command only displays information for ports with an active link (green light is on). If these conditions are not met, you can issue a show running-configuration command to confirm the configuration.

QUESTION 392:

Is the following statement True or False?
For optimal performance you should manually select the root switch.

A. False
B. True
C. There is not enough information to determine

Answer: B

Explanation:

The selection of the root switch for a particular VLAN is very important. You can choose it, or you can let the switches decide on their own. The second option is risky because there may be sub-optimal paths in your network if the root selection process is not controlled by you.

QUESTION 393:

On switch CK1 the following output was shown:
VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, address 0030.94fc.0a00
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32768, address 0001.6445.4400
Root port is 323 (FastEthernet6/3), cost of root path is 19
Topology change flag not set, detected flag not set
Number of topology changes 2 last change occurred 00:02:19 ago
from FastEthernet6/1
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers:hello 0, topology change 0, notification 0, aging 300
Port 323 (FastEthernet6/3) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 129.67.
Designated root has priority 32768, address 0001.6445.4400
Designated bridge has priority 32768, address 0001.6445.4400
Designated port id is 129.67, designated path cost 0
Timers:message age 2, forward delay 0, hold 0
Number of transitions to forwarding state:1
BPDU:sent 3, received 91
Which command could you use to reproduce the above output (Type in answer below)

Answer: show spanning-tree vlan 1

Explanation:
This example shows how to display spanning tree information for a specific VLAN:
Switch# showspanning-treevlan1
VLAN1isexecutingtheieeecompatibleSpanningTreeprotocol
BridgeIdentifierhaspriority32768,address0030.94fc.0a00
Configuredhellotime2,maxage20,forwarddelay15
Wearetherootofthespanningtree
Topologychangeflagnotset,detectedflagnotset
Numberoftopologychanges5lastchangeoccurred01:50:47ago
fromFastEthernet6/16
Times:hold1,topologychange35,notification2
hello2,maxage20,forwarddelay15
Timers:hello0,topologychange0,notification0,aging300
Port335(FastEthernet6/15)ofVLAN1isforwarding

Portpathcost19,Portpriority128,PortIdentifier129.79.
Designatedroothaspriority32768,address0030.94fc.0a00
Designatedbridgehaspriority32768,address0030.94fc.0a00
Designatedportidis129.79,designatedpathcost0
Timers:messageage0,forwarddelay0,hold0
Numberoftransitionstoforwardingstate:1
BPDU:sent6127,received0
Switch#
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_12/cmdref/show1.htm#30158

QUESTION 394:

What command would you enter if you wanted to display the current state of the spanning tree for the "vlan_id" entered from the perspective of the switch on which it is entered?

A. show spantree id vlan_id
B. show spantree vlan_id state
C. show spantree vlan_id
D. show spantree state vlan_id
E. show spantree vlan vlan_id

Answer: C

Explanation:
Commands to Use for Verifying the Configuration is Working:
show spantree vlan_id - Shows the current state of the spanning tree for the "vlan_id" entered from the perspective of the switch on which it is entered.

QUESTION 395:

You want to load balance traffic across your LAN. Which of the methods below are NOT the valid ways to configure load sharing with trunk ports? (Select all that apply)

A. using STP vector metrics
B. using ISL VLAN
C. using STP path costs
D. using STP port priorities
E. using STP SID

Answer: A, B, E

Explanation:
Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To

avoid loops, Spanning-Tree Protocol (STP) normally blocks all but one parallel link between switches. With load sharing, you divide the traffic between the links according to which VLAN the traffic belongs to. There are two ways to configure load sharing by using trunk ports: using STP port priorities or using STP path costs.
Incorrect Answers:
C: If you configure load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.
D: If you configure load sharing using STP port priorities, both load-sharing links must be connected to the same switch.

QUESTION 396:

What switch characteristic(s), aside from the MAC address, determines which switch will become the root bridge (Select all that apply)?

A. IP address
B. The port cost
C. Path cost
D. Priority number
E. The port ID

Answer: D

Explanation:
When you configure a switch as the secondary root, the spanning-tree bridge priority is modified from the default value (32768) to 16384 so that the switch is likely to become the root for the specified VLANs if the primary root switch fails (assuming the other switches in the network use the default bridge priority of 32768). The MAC address is also used in the determination as a tie-breaker if two switches have the same priority value.
Note: In STP, lower is better, meaning that the lower bridge priority is preferred over a higher value.

QUESTION 397:

In a CLI based switch, what command will display the information comparable to the IOS command "show span"? (Type in answer below)

Answer: show spantree

Explanation:
Use the show spantree command to display spanning-tree information for a VLAN.
show spantree [vlan | mod_num/port_num] [active]vlan (Optional) Number of the VLAN. If the VLAN number is not specified, the default is VLAN 1.
mod_num (Optional) Number of the module.

port_num (Optional) Number of the port on the module.
active (Optional) Keyword that specifies to display only the active ports.

QUESTION 398:

You are a network troubleshooter, and you've arrived at a jobsite to troubleshoot a Catalyst 5000 switch. After talking with the system administrator you come to suspect that the Root Bridge for VLAN 1 is incorrect. Which command would you enter at the CLI to determine VLAN 1's root bridge?

A. show span 1
B. show spantree
C. show bridge vlan 1
D. show spantree root bridge
E. None of the above

Answer: B

Explanation: By default the show spantree command displays the STP information for VLAN 1. The bridge ID, MAC address, and timers are displayed.
Sample output:
Certkiller > (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type ieee
Designated Root 00-d1-22-24-56-00
<Rest of output deleted>
The Designated Root value in the output is the MAC address of the root bridge.

QUESTION 399:

Which command would you enter to display the blocked ports on a spanning tree environment? (Type in answer below)

Answer: show spantree blockedports

Explanation:
Use the show spantree blockedports command to display only the blocked ports.
show spantree blockedports [vlan_num]vlan_num (Optional) Number of the VLAN.
The following list various commands to use for troubleshooting Catalyst switches:
show spantree vlan_id - Shows the current state of the spanning tree for the "vlan_id" entered from the perspective of the switch on which it is entered.
show spantree summary - Provides a summary of connected spanning tree ports by VLAN.
show spantree statistics - Shows spanning tree statistical information.
show spantree backbonefast - Displays whether the spanning tree Backbone Fast

Convergence feature is enabled.
show spantree blockedports - Displays only the blocked ports.
show spantree portstate - Determines the current spanning tree state of a Token Ring port within a spanning tree.
show spantree portvlancost - Shows the path cost for the VLANs on a port.
show spantree uplinkfast - Shows the uplinkfast settings.

QUESTION 400:

You have a congested Ethernet network with only one Root Bridge on the Certkiller network. What can you do to reduce BPDU traffic on this network?

A. Remove redundant links between switches
B. Decrease the MaxAger timer on all non-Root Bridges
C. Increase the BPDU Hello timer only on the Root Bridge
D. Increase the Path Cost on the Designated Port on all non-Root Bridges

Answer: C

Explanation:
There are several STP timers, as listed below:
1. hello: the hello time is the time between each Bridge Protocol Data Unit (BPDU) that is sent on a port. This is equal to two seconds by default, but can be tuned to be between one and ten seconds.
2. forwarddelay: the forward delay is the time spent in the listening and learning state. This is by default equal to 15 seconds, but can be tuned to be between four and 30 seconds.
3. maxage: the max age timer controls the maximum length of time a bridge port saves its configuration BPDU information. This is 20 seconds by default and can be tuned to be between six and 40 seconds.
The STP timers (hello, forward delay, and max age) are included in each BPDU. An IEEE bridge is not concerned about its local configuration of the timers value.
To reduce BPDU traffic on this network, increase these timers.
Incorrect Answers:
A: Redundant links are not used when STP is in use. STP will block these redundant links automatically.
B: This will be counterproductive, as it will increase the number of BPDU's
D: This will have no effect on the BPDU traffic.

QUESTION 401:

While logged in to switch Certkiller 1 you see the following output:
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state.
Which action could have caused the following output to appear on a switch?

A. The switch is configured with Loop Guard and stops receiving BPDUs.
B. The switch is configured with PortFast and starts receiving BPDUs
C. The switch is configured with Loop Guard and stops receiving superior BPDUs
D. The switch is configured with Loop Guard and starts receiving inferior BPDUs

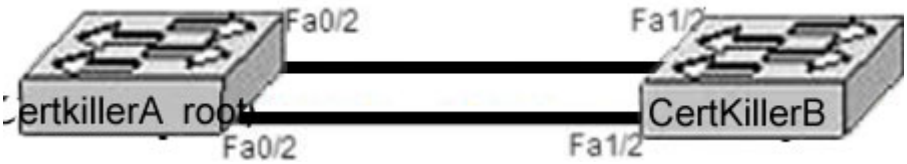
Answer: C

Explanation:
The loop guard is intended to provide additional protection against L2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) stopped receiving STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs, depending on the port role (designated port transmits, non-designated port receives BPDUs).
When one of the ports in a physically redundant topology stops receiving BPDUs, the STP conceives the topology as loop free. Eventually, the blocking port from the alternate or backup port becomes designated, and moves to forwarding state, thus creating a loop.
With the loop guard, an additional check is made. If BPDUs are not received any more on a non-designated port and the loop guard is enabled, that port will be moved into the STP loop-inconsistent blocking state instead of moving to the listening / learning / forwarding state. Without the loop guard, the port would assume the designated port role. The port would move to STP forwarding state, and thus create a loop.
When the loop guard blocks an inconsistent port, the following message is logged.
SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to loop-inconsistent state.
Once the BPDU is received on a port in a loop-inconsistent STP state, the port will transition into another STP state. According to the received BPDU, this means that the recovery is automatic, and no intervention is necessary. After the recovery, the following message is logged.
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
Reference:
http://www.cisco.com/en/US/tech/ CK3 89/ CK6 21/technologies_tech_note09186a0080094640.shtml#feature

---

QUESTION 402:

Exhibit



Assuming that VLAN 1 and VLAN 2 traffic is enabled on the above network, what effect will the following command have when entered on port 0/2 on switch Certkiller A?

spanning-tree vlan 1 port-priority 16

A. VLAN 1 traffic will be blocked on Switch Certkiller B port 1/1.
B. VLAN 2 traffic will be blocked on Switch Certkiller B port 1/1.
C. VLAN 2 traffic will be blocked on Switch Certkiller A port 0/2.
D. VLAN 1 and 2 traffic will be blocked on Switch Certkiller A port 0/1.
E. VLAN 1 and 2 traffic will be blocked on Switch Certkiller A port 0/2.

Answer: A

QUESTION 403:

You are a network troubleshooter, and you've just been contracted by Certkiller Inc. to troubleshoot their switched network, which just suddenly started experiencing difficulties after a junior administrator added a switch named Test1 to the network.
1. Their network runs on a VTP domain called 'main1'.
2. The network has the active VLANs 1,2,3,4,5,10, & 20.
3. No traffic is being passed on VLANs 2,3,4,5,10, &20 (which means the switches are working)
What are the configuration issues on the new switch that could be responsible for the network outage? (Select all that apply)

A. TEST1 is configured as a VTP server with a different domain name.
B. TEST1 is not configured to participate in VTP.
C. TEST1 is configured as a VTP server with the domain name main1.
D. TEST1 has a lower VTP configuration revision than the current VTP revision.
E. TEST1 has a higher VTP configuration revision than the current VTP revision.
F. TEST1 is configured with only VLAN1.

Answer: C, E, F

Explanation:
If a VTP server with the same name is added to the VTP domain (C), and the configuration revision number is higher (E), all other switches in the domain will synchronize with the highest
number and take on that configuration (F), only VLAN1. In this case, if the new VTP server is added to the network and is only configured with VLAN1, this information will be propagated throughout the network and will delete the other VLANs.

QUESTION 404:

Which protocol is an extension to ICMP that provides a mechanism for routers to advertise useful default routes?

A. IRDP

B. HSRP
C. VRRP
D. Proxy ARP
E. GLBP

Answer: A
IRDP is an extension to ICMP that provides a mechanism for routers to advertise useful default routes

---

QUESTION 405:

Which IOS command could you use to confirm whether or not routing is enabled on router CK1 ?

A. Switch(config)#ip routing
B. Switch#show ip routing
C. Switch(config)#routing
D. Switch#show routing

Answer: B

Explanation:
Use the show ip routing command in EXEC mode to display the current state of the IP routing protocols being routed.

QUESTION 406:

Is the following statement True or False?
MLS requires that the router have a path to each of the VLANs on the network.

A. There is not enough information to determine
B. False
C. True

Answer: C

Explanation:
It is a basic topology requirement of MLS that the router have a path to each of the VLANs. Remember that the point of MLS is to create a shortcut between two VLANs, so that the "routing" between the two end devices can be performed by the switch, thus freeing the router for other tasks.The switch is not actually routing; it is rewriting the frames so that it appears to the end devices that they are talking through the router. If the two devices are in the same VLAN, then the MLS-SE will switch the frame locally without utilizing MLS, as switches do in such a transparently bridged environment, and no MLS shortcut will be created. One can have multiple switches and routers in the network, and even multiple switches along the flow path, but the path between the two

end devices for which one desires an MLS shortcut must include a single MLS-RP in that VLAN for that path. In other words, the flow from source to destination must cross a VLAN boundary on the same MLS-RP, and a candidate and enabler packet pair must be seen by the same MLS-SE for the MLS shortcut to be created. If these criteria are not met, then the packet will be routed normally without the use of MLS.

QUESTION 407:

The CEO of your company, Certkiller, is complaining about slow network performance on her workstation. While applying your systematic Cisco troubleshooting approach you clear the counters and issue the show port command which indicate to you a high number of alignment and FCS errors. What is potentially causing Jack's problem?

A. There is a speed mismatch.
B. There is a duplex mismatch.
C. There is a trunk mode mismatch.
D. There is a VTP mode mismatch.

Answer: B

Explanation:
The show port command is used to display port status and counters. Alignment and FCS errors are frames that do not end with an even number of octets and have a bad CRC. This indicates that a valid connection exists but that there are corrupt frames. This could be caused by a duplex mismatch.
Incorrect Answers
A: A speed mismatch cannot be the cause of the problem. The speed would automatically be configured to the highest common speed.
C: A trunk mode mismatch would not allow transfers of any frames at all.
D: A VTP mode mismatch would not allow transfers of any frames at all.

QUESTION 408:

What kinds of losses are observed on healthy networks during brief periods of congestion?

A. Loss due to jitter.
B. Loss due to delay.
C. Loss due to noise.
D. Loss due to deliberately dropped packets.

Answer: D

Explanation:
When a network becomes too congested, some network devices deliberately drop some

packets to maintain flow. Most of these packets are TCP/IP file and print services, so if a few packets are dropped there's no major concern. However, if a UDP packet of a video or voice transaction gets dropped, there's a concern. To address this, some congestion avoidance methods were implemented that are supported by Cisco devices, such as RED and WRED.

QUESTION 409:

In the three-Layer hierarchical network design model; associated with the access layer? (Select two)

A. optimized transport structure
B. high port density
C. boundary definition
D. data encryption
E. local VLANs
F. route summaries

Answer: B, E

Explanation:
The access layer is the outermost layer, and it is composed of the least sophisticated network equipment. The most important function of the access layer is high port density, since these devices connect the individual end users. The access layers are also where VLANs are implemented, since VLANs are assigned on a per-port basis.

QUESTION 410:

You are a system administrator and you've recently implemented 'tail drops' on your network as a congestion avoidance mechanism. Which QoS technique can you use to avoid the potential problems caused by tail drops?

A. CAR
B. WRED
C. CBWFQ
D. RSVP

Answer: B

Explanation:
With class-based QoS queuing, you can create up to 64 classes for an interface. (Unlike WFQ, queues are not automatically based on the packet's ToS value.) Class-based QoS queuing also lets you control the drop mechanism used when congestion occurs on the interface. You can use WRED for the drop mechanism, and configure the WRED queues, to ensure that high-priority packets within a class are given the appropriate weight. If you use tail drop, all packets within a class are treated equally, even if the ToS values are not

equal.
Reference:
www.cisco.com/en/US/products/sw/cscowork/ps2064/products_user_guide_chapter09186a00800e0a04.html

---

QUESTION 411:

The Certkiller network is utilizing QoS techniques to prioritize their mission critical data. What's true about implementing QoS at the access, distribution, and core layers? (Select two)

A. QoS implementation is the same for the access, distribution, and core layers.
B. Classification and Marking should be done at the access layer.
C. No QoS mechanisms are configured at the access layer since access layer switches like the Catalyst 2950 are not QoS capable.
D. The high speed core layer only requires proper queuing (like LLQ) and dropping (like WRED) configurations.

Answer: B, D

Explanation:
You typically want to classify and mark traffic as close to source as possible (typically access layer unless you have server farms that are grouped at distribution layer). In addition, the network core should be designed to process and pass data as quickly as possible, without the added overhead of QoS configurations.
Incorrect Answers:
A: QoS markings are typically performed on the access layer, with some additional QoS mechanisms used at the distribution layer in many cases. In the core of the network, QoS should be avoided.
C: This is not true, as a number of QoS capabilities exist on these access layer switches.

QUESTION 412:

In the three-layer hierarchical network design model, what's associated with the core layer? (Select two)

A. Access control list
B. Data encryption
C. Optimized transport
D. Address aggregation
E. Packet switching
F. Boundary definition

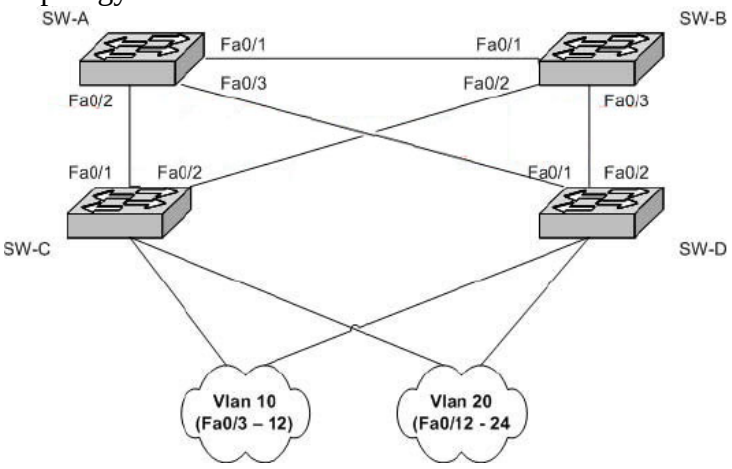
Answer: C, E

Explanation:
A hierarchical network design includes the following three layers:

-The backbone (core) layer that provides optimal transport between sites
-The distribution layer that provides policy-based connectivity
-The local-access layer that provides workgroup/user access to the network
The distribution layer of the network is the demarcation point between the access and core layers and helps to define and differentiate the core. The purpose of this layer is to provide boundary definition and is the place at which packet manipulation can take place. In the campus environment, the distribution layer can include several functions, such as the following:
Address or area aggregation
1. Departmental or workgroup access
2. Broadcast/multicast domain definition
3. Virtual LAN (VLAN) routing
4. Any media transitions that need to occur
5. Security
The distribution layer can be summarized as the layer that provides policy-based connectivity
Reference: www.alteridem.net/networking/idg4/idgbasic.htm

Case Study Certkiller .com, Scenario

Certkiller .com is an Internet game provider. The game service network had recently added an additional switch block with multiple VLANs configured. Unfortunately, system administrators neglected to document the Spanning-Tree topology during configuration. For baseline purposes, you will be required to identify the Spanning-Tree topology for the switch block. Using the show output of the command show spanning-tree on switch SW-C and the provided physical topology, answer the following questions:
Topology:



Output:

```
SW-C# show spanning-tree

VLAN0001
Spanning tree enabled protocol rstp
Root IP  Priority   32769
         Address         000d.65db.9800
         Cost            19
         Port            1 (FastEthernet0/1)

         Address         000d.bd03.27c0
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
         Aging Time 300

Interface        Role  Sts  Cost  Prio.Nbr  Type
Fa0/1            Root  FWD  19    128.1     P2p
Fa0/2            Desg  FWD  19    128.1     P2p Peer (STP)

VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 24586
         Address         000f.34f5.2400
         Cost            19
         Port            2 (FastEthernet0/29
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority 32788 (priority 32768 sys-id-ext 20)
         Address         000d.bd03.27c0
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
         Aging Time 300
Interface        Role  Sts  Cost  Prio.Nbr  type
Fa0/1            Root  FWD  19    128.1     P2p
Fa0/2            Desg  FWD  19    128.1     P2p Peer (STP)
```

Case Study Certkiller .com (5 Questions)

QUESTION 413:

For VLANs 1 and 10, in which port state is interface Fa0/2 of switch SW-B?

A. blocking
B. disabled
C. discarding
D. forwarding
E. learning

Answer: A

QUESTION 414:

Which bridge ID belongs to switch SW-A?

A. 24586.000f.34f5.2400
B. 32768.000d.bd03.27c0
C. 32768.000d.65db.9800

D. 32769.00d.65db.9800
E. 32788.000d.bd03.27c0

Answer: D

QUESTION 415:

Which bridge ID belongs to switch SW-B?

A. 24586.000f.34f5.2400
B. 32768.000d.bd03.27c0
C. 32768.000d.65db.9800
D. 32769.00d.65db.9800
E. 32788.000d.bd03.27c0

Answer: A

QUESTION 416:

Exhibit: **MISSING **
Which Spanning Tree Protocol has been implemented on switch SW-B?

A. PVST+
B. PVRST
C. MSTP/IEEE 802.1s
D. STP/IEEE 802.1D

Answer: A

QUESTION 417:

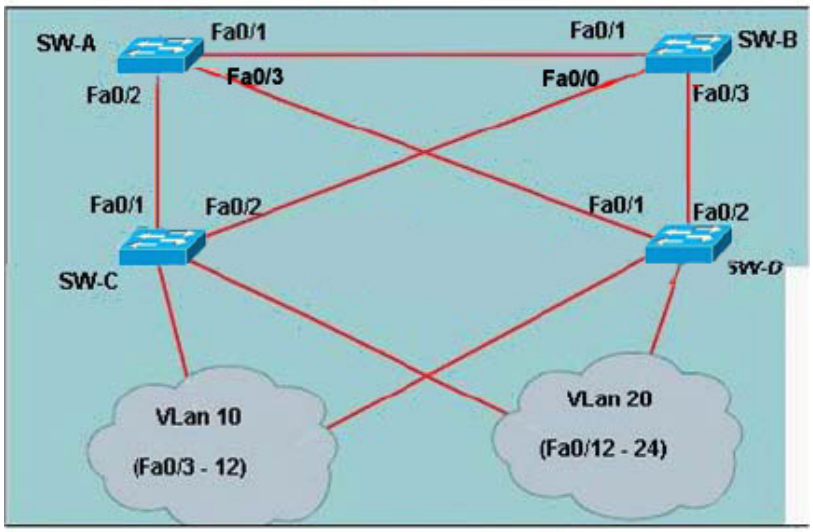
Which port role has interface Fa0/2 of switch SW-A adopted for VLAN 20?

A. alternate port
B. backup port
C. designated port
D. root port
E. nondesignated port

Answer: C

Case Study Certkiller , Scenario

Exhibit:



SW-C# shows panning-tree

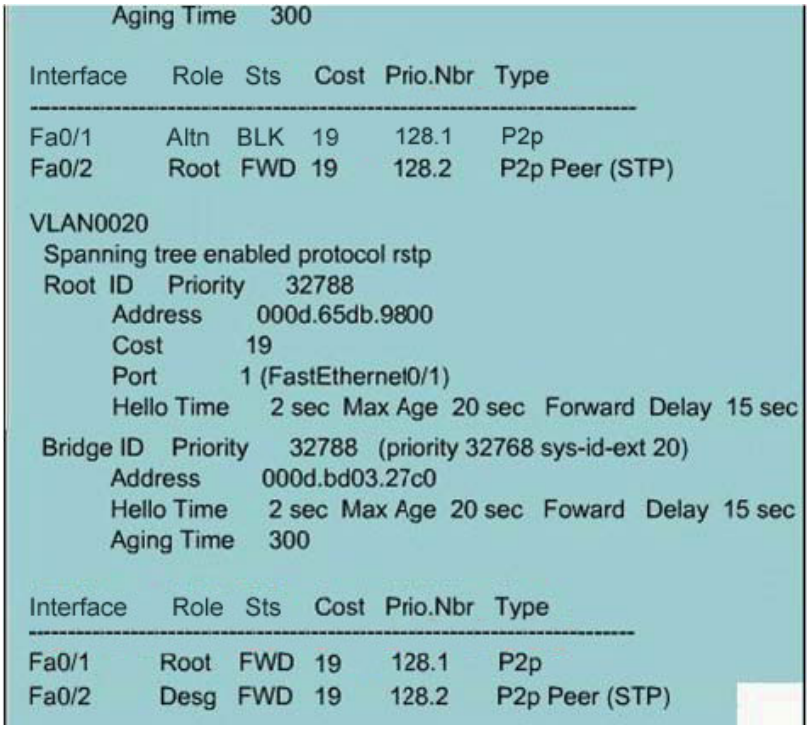
```
VLAN0001
 Spanning tree enabled protocol rstp
 Root ID  Priority    32769
        Address     000d.65db.9800
        Cost        19
        Port        1 (FastEthernet0/1)
        Hello Time   2 sec  Max Age  20 sec  Forward Delay 15 sec

 Bridge ID  Priority   32769  (priority 32768 sys-id-ext 1)
        Address   000d.bd03.27c0
        Hello Time  2 sec  Max  Age  20 sec  Foward  Delay  15 sec
        Aging Time  300

Interface     Role  Sts   Cost  Prio.Nbr  Type
-------------------------------------------------------------------
Fa0/1         Root  FWD 19      128.1     P2p
Fa0/2         Desg  FWD 19      128.2     P2p Peer (STP)


VLAN0010
 Spanning tree enabled protocol rstp
 Root ID    Priority    24586
        Address     000f.34f5.2400
        Cost        19
        Port        2 (FastEthernet0/2)
        Hello Time   2 sec  Max Age  20 sec  Forward  Delay  15 sec

 Bridge ID Priority    32 73  (priority 32738sys-d.ext10)
        Address     000d.bd03.27c0
        Hello Time   2 sec  Max Age  20 sec  Foward  Delay  15 sec
```



```
        Aging Time   300

Interface     Role  Sts   Cost  Prio.Nbr  Type
---------------------------------------------------------------------
Fa0/1         Altn  BLK   19    128.1     P2p
Fa0/2         Root  FWD   19    128.2     P2p Peer (STP)

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID    Priority    32788
         Address      000d.65db.9800
         Cost         19
         Port         1 (FastEthernet0/1)
         Hello Time   2 sec  Max Age  20 sec  Forward  Delay  15 sec
  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
         Address      000d.bd03.27c0
         Hello Time   2 sec  Max Age  20 sec  Foward   Delay  15 sec
         Aging Time   300

Interface     Role  Sts   Cost  Prio.Nbr  Type
---------------------------------------------------------------------
Fa0/1         Root  FWD   19    128.1     P2p
Fa0/2         Desg  FWD   19    128.2     P2p Peer (STP)
```

Certkiller .com is an Internet game provider, the game service network had recently added an additional switch block with multiple VLANS configured. Unfortunatley, system administrator neglected to document the Spanning-Tree topology and configuration. For baseline purposes, you will be required to identify the Spanning-Tree topology for the switch block. Using the show output of the command show spanning-tree on switch SW-C and the provided physical topology, answer the following questions:

Case Study Certkiller , Questions (5 Questions)

QUESTION 418:

Which bridge ID belongs to switch SW-A?

A. 24586.000f.34f5.2400
B. 32768.000d.bd03.27c0
C. 32768.000d.65db.9800
D. 32769.000d.65db.9800
E. 32788.000d.bd03.27c0

Answer: D

QUESTION 419:

Which bridge ID belongs to switch SW-B?

A. 24586.000f.34f5.2400

B. 32768.000d.bd03.27c0
C. 32768.000d.65db.9800
D. 32769. 000d.65db.9800
E. 32788.000d.bd03.27c0

Answer: A

QUESTION 420:

Which Spanning Tree Protocol has been implemented on switch SW_B?

A. PVST+
B. PVRST
C. MSTP/IEEE 802.1s
D. STP/IEEE 802.1D

Answer: A

QUESTION 421:

For VLANs 1 and 10, in which port state is interface Fa0/2 of switch SW-B?

A. Blocking
B. Disabled
C. Discarding
D. Forwarding
E. learning

Answer: A

QUESTION 422:

Which port has interface Fa0/2 of switch SW-A adopted for VLAN 20?

A. Alternate port
B. Backup port
C. Designated port
D. Root port
E. Nondesignated port

Answer: C

Mixed Questions (42 Questions)

QUESTION 423:

A network administrator wants to permit only SSH access to a Cisco IOS device.
Which line configuration command will accomplish this?

A. access-class ssh in
B. access-group ssh in
C. access-class ssh out
D. transport input all
E. transport input ssh

Answer: E

Explanation: If you want to prevent non-SSH connections, add the transport input ssh command under the lines to limit the router to ssh connections only. By default router allows all connections.

QUESTION 424:

Which three IP addresses are valid multicast addresses? (Choose three.)

A. 169.254.23.59
B. 223.254.255.254
C. 225.1.1.1
D. 227.43.34.2
E. 238.3.3.3
F. 249.1.2.3

Answer: C, D, E

Explanation:
Routers and switches must have a way to distinguish multicast traffic from unicasts or broadcasts. This is done through IP addressing, by reserving the Class D IP address range, 224.0.0.0 through 239.255.255.255, strictly for multicasting. Network devices can quickly pick out multicast IP addresses by looking at the four most-significant bits, which are always 1110.
Some of the IP multicast address space has been reserved for a particular use:
_ Completemulticast space: 224.0.0.0 through 239.255.255.255-The entire range of IP addressesthat can be used for multicast purposes.
_ Link-local addresses (224.0.0.0 through 224.0.0.255)-Used by network protocols only on thelocal network segment. Routers do not forward these packets.
This space includes the all-hosts address 224.0.0.1, all-routers 224.0.0.2, OSPF-routers 224.0.0.5, and so on. These are also known as fixed-group addresses because they are wellknown andpredefined.
_ Administrativelyscoped addresses (239.0.0.0 through 239.255.255.255)-Used in private multicastdomains, much like the private IP address ranges from RFC 1918. These addresses arenot routed between domains, so they can be reused.
_ Globallyscoped address(224.0.1.0through 238.255.255)-Used by any entity;these addressescan be routed across an organization or the Internet, so they must be unique and

globallysignificant.(Think of this range as either local nor private ;it is rest of the multicast range.)
So Answer C,D and E are correct.

QUESTION 425:

Which three statements are true about the Internet Group Management Protocol (IGMP)? (Choose three.)

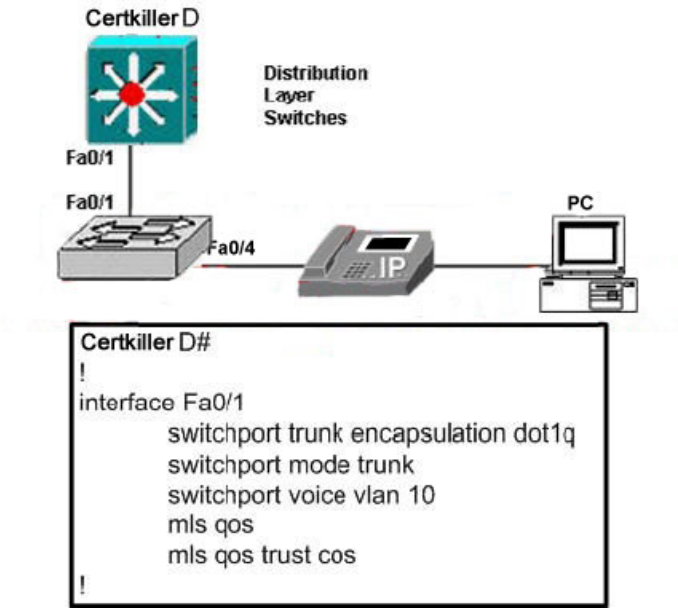
A. IGMP is a multicast routing protocol that makes packet-forwarding decisions independent of other routing protocols such as EIGRP.
B. IGMP is used to register individual hosts with a multicast group.
C. IGMP messages are IP datagrams with a protocol value of 2, destination address of 224.0.0.2, and a TTL value of 1.
D. IGMP snooping runs on Layer 3 routers.
E. IGMP version 3 enables a multicast receiving host to specify to the router which sources it should forward traffic from.
F. There are three IGMP modes: dense mode, sparse mode, and sparse-dense mode.

Answer: B, C, E

Explanation:
A host can join a multicast group by sending a request to its local router. This is done through the Internet Group Management Protocol (IGMP). IGMPv1 is defined in RFC 1112, and its successor, IGMPv2, in RFC 2236.When several hosts join a group by contacting their local routers, it is the multicastrouting protocol (such as PIM) that "connects the dots" and forms the multicast tree betweenrouters.
In addition, hosts are allowed to leave a group dynamically. When a host decides to leave a group it hasjoined, it sends a Leave Group message to the all-routers address (224.0.0.2). All routers on the localsegment take note, and the Querier router decides to investigate further.

QUESTION 426:

Exhibit:



Refer to the exhibit. A trunk link is connected between switch Certkiller A and switch Certkiller D. Based on the configuration shown in the exhibit, how would the traffic coming from the switch Certkiller A be managed?

A. The trunk port Fa0/1 on switch Certkiller A will trust all CoS values on the frames coming from the IP phone.
B. The trunk port Fa0/1 on switch Certkiller A will trust all CoS values on the frames received on the IP phone.
C. The trunk port Fa0/1 on switch Certkiller D will trust all CoS values on the frames coming from port Fa0/1 on Certkiller A.
D. The trunk port Fa0/1 on switch Certkiller D will trust all CoS values on the frames received on the Certkiller A switch port Fa0/4.
E. The trunk port Fa0/1 on switch Certkiller D will trust all CoS values on the frames received on the IP phone port.

Answer: C

Explanation:
To enable to QOS, you should enter the msl qos command in global configuration mode.
When inbound packets are accepted into a switch, the switch can be selective about which (if any) ofeach packet's QoS information will be trusted. If the packets originate from a trusted source, the QoSinformation can be safely trusted, too. Usually, it is a best practice to configure switches at theedge of a trusted QoS domain to verify or overwrite any QoS information that comes into the domain. This way, any other switch or router within the domain can blindly trust QoS information thatis seen.
You can configure QoS trust in two ways:
1. Per-interface
2. As part of a QoS policy on specific types of traffic
The per-interface trust is described in the next section. Policy trust is described as part of the section,

"Defining a QoS Policy."
Trust QoS on an Interface
On each interface where consistent QoS trust is to be defined, use the following interface configurationcommand:
Switch(config-if)# mls qos trust {cos | dscp| ip-precedence}
Applying QoS Trust 407
Here, one of the following values can be trusted and used internally as the switch makes forwarding decisions:
1. The inbound CoS, which is taken from trunking tags
2. DSCP, which is taken from the inbound IP packet headers
3. IP Precedence, which is also taken from the inbound IP packet headers

---

QUESTION 427:

Exhibit:


```
Certkiller1#show running-config

----output omitted----

interface FastEthernet0/13
description Trunk to  Certkiller2
switchport trunk encapsulation isl
switchport trunk allowed vlan 10
switchport mode trunk
speed 100
!
Interface FastEthernet0/14
description Trunk to  Certkiller2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 20,30,50,60,700,800,3000
switchport mode trunk
speed 100
```

```
Certkiller1#show running-config

----output omitted----

interface FastEthernet0/13
description Trunk to  Certkiller1
switchport trunk encapsulation isl
switchport trunk allowed vlan 10
switchport mode trunk
speed 100
!
Interface FastEthernet0/14
description Trunk to  Certkiller1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 20,30,50,60,700,800,3000
switchport mode trunk
speed 100
```

Refer to the exhibit. Given these configurations, what is true about interfaces FastEthernet0/13 and 0/14 on Certkiller 2?

A. Interface Fa0/13 is up, but Fa0/14 is down because of trunk encapsulation incompabilities.
B. Interface Fa0/13 is down, but Fa0/14 is up because of trunk encapsulation incompabilities.
C. Interface Fa0/13 and Fa0/14 are both down because of trunk encapsulation incompabilities.
D. Interface Fa0/13 and Fa0/14 are both up.

Answer: D

Explanation: Answer D is correct because, both interface of Certkiller 1 and Certkiller 2 have similar encapsulation, speed and vtp mode.

QUESTION 428:

Which two statements are true about Internet Group Management Protocol (IGMP) snooping? (Choose two.)

A. IGMP snooping and Cisco Group Membership Protocol (CGMP) can be used simultaneously on a switch.
B. IGMP snooping and Cisco Group Membership Protocol (CGMP) were developed to help Layer 3 switches make intelligent forwarding decisions on their own.
C. IGMP snooping examines IGMP join/leave messages so that multicast traffic is forwarded only to hosts that sent an IGMP message towards the router.
D. IGMP snooping is an IP multicast constraining mechanism for Layer 2 switches.
E. IGMP snooping is enabled with the ip multicast-routing global configuration command.

Answer: C, D

Explanation:
IGMP version 2 introduced several differences from the first version. Queries can be sent as General Queries to the all-hosts address (as in IGMPv1), as well as Group-Specific Queries, sent only to membersof a specific group.
In addition, hosts are allowed to leave a group dynamically. When a host decides to leave a group it hasjoined, it sends a Leave Group message to the all-routers address (224.0.0.2). All routers on the localsegment take note, and the Querier router decides to investigate further. It responds with a Group-Specific Query message, asking if anyone is still interested in receiving traffic for that group. Any other hosts must reply with a Membership Report. Otherwise, the Querier safely assumes that thereis no need to continue forwarding the group traffic on that segment.

QUESTION 429:

Which command will enable the 802.1Q trunking encapsulation on a trunk?

A. switchport mode trunk
B. switchport trunk encapsulation dot1q
C. switchport encapsulation 802.1q
D. switchport mode trunk dot1q
E. switchport trunk native

Answer: B

Explanation:
A trunk link, however, can transport more than one VLAN through a single switch port. Trunk links aremost beneficial when switches are connected to other switches or switches are connected to routers. A trunk link is not assigned to a specific VLAN. Instead, one, many, or all active VLANs canbe transported between switches using a single physical trunk link.
VLAN identification can be performed using two methods, each using a different frame identifier mechanism:
1. Inter-Switch Link (ISL) protocol
2. IEEE 802.1Q protocol

Example:
Switch(config-if)# switchport trunk encapsulation {isl | dot1q | negotiate}

QUESTION 430:

Exhibit:

```
CK2#show running-config

-----output omitted-----

aaa new-model
aaa authentication dot1x default group radius
dot1x system-auth-control

-----output omitted-----

interface fastethernet 0/6
dot1x port-control auto
```

Refer to the exhibit. Which statement is true about the show running-config output?

A. CK2 is configured for switch-based authentication using RADIUS.
B. Interface FastEthernet0/6 is configured with a SmartPort macro using RADIUS.
C. Interface FastEthernet0/6 is configured for 802.1X Authenticated Trunking Protocol (ATP).
D. Interface FastEthernet0/6 is configured for port-based traffic control.
E. Interface FastEthernet0/6 is configured for port-based authentication.

Answer: E

Explanation:
Catalyst switches can support port-based authentication, a combination of AAA authentication and portsecurity. This feature is based on the IEEE 802.1x standard.
For port-based authentication, both the switch and the end -user's PC must support the 802.1x standard,
usingthe Extensible Authentication Protocol over LANs (EAPOL). The 802.1x standard is a cooperativeeffort between the client and the switch offering network service. If the client PC is configuredto use 802.lx but the switch does not support it, the PC abandons the protocol and communicates
normally. However, if the switch is configured for 802.1x but the PC does not support it, the switchport remains in the unauthorized state so that it will not forward any traffic to the client PC.
Example
Switch(config)# dot1x system-auth-control
You must configure each switch port that will use 802.1x. Use the following interface configuration commandto set the authentication state:
Switch(config-if)# dot1x port-control {force-authorized | force-unauthorized | auto}

QUESTION 431:

Which two ACL types can be used on a Catalyst 3550 switch to filter traffic?
(Choose two.)

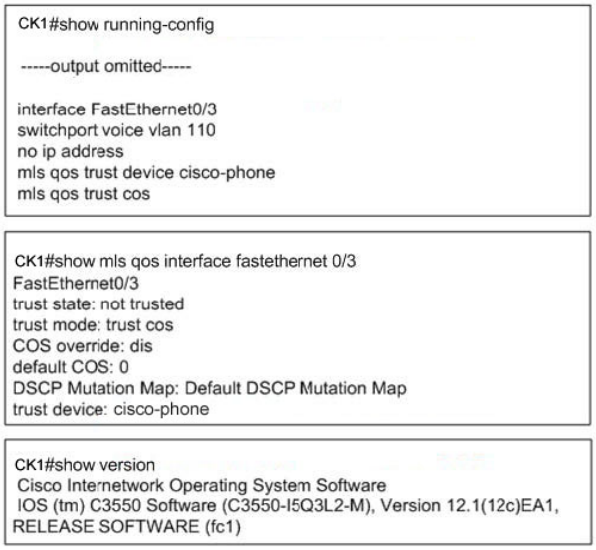
A. CBAC
B. VLAN Maps
C. Router ACLs
D. Reflexive ACL

Answer: B, C

Explanation:
VACLsare configured as a VLAN access map, in much the same format as a route map. A VLAN accessmap consists of one or more statements, each having a common map name. First, you define theVACL with the following global configuration command:
Switch(config)# vlan access-map map-name [sequence-number]
Access map statements are evaluated in sequence, according to the sequence-number. Each statementcan contain one or more matching conditions, followed by an action.
Example:
Switch(config)# ip access-list extended local-17
Switch(config-acl)# permit ip host 192.168.99.17 192.168.99.0 0.0.0.255
Swtich(config-acl)# exit
Switch(config)# vlan access-map block-17 10
Switch(config-access-map)# match ip address local-17
Switch(config-access-map)# action drop
Switch(config-access-map)# vlan access-map block-17 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter block-17 vlan-list 99
Another ACL type can be used on catalyst 3550 switch is Router ACL.

QUESTION 432:

Exhibit:



Refer to the exhibit. Why does the trust state of interface FastEthernet 0/3 show "not trusted"?

A. DSCP map needs to be configured for VOIP.
B. ToS has not been configured.
C. ToS has been misconfigured.
D. The command mls qos needs to be turned on in global configuration mode.
E. There is not a Cisco Phone attached to the interface.

Answer: E

Explanation:
To verify how QoS trust has been extended to the IP Phone itself, use the following EXEC command:
Switch# show mls qos interface type mod/num
If the port is trusted, all traffic forwarded by the IP Phone is accepted with the QoS information left intact. If the port is not trusted, even the voice packets can have their QoS information overwritten bythe switch. See the example output :
Switch# show mls qos interface fast 0/1
FastEthernet0/1
truststate: trust cos
trustmode: trust cos
COS override: dis
defaultCOS: 0
DSCP Mutation Map: Default DSCP Mutation Map
trustdevice: none
Configuration is correct but the trust state is not trusted so no Cisco phone is attached to the interface.

QUESTION 433:

What will occur when a nonedge switch port that is configured for Rapid Spanning

Tree does not receive a BPDU from its neighbor for three consecutive hello time intervals?

A. RSTP information is automatically aged out.
B. The port sends a TCN to the root bridge.
C. The port moves to listening state.
D. The port becomes a normal spanning tree port.

Answer: A

Explanation:
The IEEE 802.1D Spanning Tree Protocol was designed to keep a switched or bridged network loop free, with adjustments made to the network topology dynamically. A topology change typically takes30 seconds, where a port moves from the Blocking state to the Forwarding state after two intervalsof the Forward Delay timer. As technology has improved, 30 seconds has become an unbearablelength of time to wait for a production network to failover or "heal" itself during a problem.
The IEEE 802.1w standard was developed to take 802.1D's principle concepts and make the resultingconvergence much faster. This is also known as the Rapid Spanning Tree Protocol (RSTP). RSTP defines how switches must interact with each other to keep the network topology loop free, ina very efficient manner. Like 802.1D, RSTP's basic functionality can be applied as a single or multipleinstances. This can be done as the IEEE 802.1s Multiple Spanning Tree (MST), covered in thischapter, and also as the Cisco-proprietary, Rapid Per-VLAN Spanning Tree Protocol (RPVST+). RSTP operates consistently in each, but replicating RSTP as multiple instances requires different approaches.
In 802.1D, BPDUs basically originate from the Root Bridge and are relayed by all switches down throughthe tree. It is because of this propagation of BPDUs that 802.1D convergence must wait for steady-stateconditions before proceeding.
RSTP uses the 802.1D BPDU format for backward-compatibility. However, some previously unusedbits in the Message Type field are used. The sending switch port identifies itself by its RSTP roleand state. The BPDU version is also set to 2, to distinguish RSTP BPDUs from 802.1D BPDUs. Also, RSTP uses an interactive process so that two neighboring switches can negotiate state changes. Some BPDU bits are used to flag messages during this negotiation.
BPDUsare sent out every switch port at Hello Time intervals, regardless of whether BPDUs are receivedfrom the Root. In this way, any switch anywhere in the network can play an active role in maintainingthe topology. Switches can also expect to receive regular BPDUs from their neighbors. When three BPDUs are missed in a row, that neighbor is presumed to be down, and all information relatedto the port leading to the neighbor is immediately aged out. This means that a switch can detecta neighbor failure in three Hello intervals (default 6 seconds), versus the Max Age Timer interval(default 20 seconds) for 802.1D.
Because RSTP distinguishes its BPDUs from 802.1D BPDUs, it can coexist with switches still using802.1D. Each port attempts to operate according to the STP BPDU that is received. For example,
whenan 802.1D BPDU (version 0) is received on a port, that port begins to operate according tothe 802.1D rules. However, each port has a measure that locks the protocol in use for the duration

ofthe migration delay timer. This keeps the protocol type from flapping or toggling during a protocol migration. After the timer expires, the port is free to change protocols if needed.

QUESTION 434:

What are three possible router states of HSRP routers on a LAN? (Choose three.)

A. standby
B. established
C. active
D. idle
E. backup
F. init

Answer: A, C, F

Explanation:
Basically, each of the routers that provides redundancy for a given gateway address is assigned to a commonHSRP group. One router is elected as the primary, or active, HSRP router, another is electedas the standby HSRP router, and all the others remain in the listen HSRP state. The routers exchangeHSRP hello messages at regular intervals, so they can remain aware of each other's existence, as well as that of the active router.

QUESTION 435:

Which two statements are true about a switched virtual interface (SVI)? (Choose two.)

A. An SVI is created by entering the no switchport command in interface configuration mode.
B. An SVI is created for the default VLAN (VLAN1) to permit remote switch administration by default.
C. An SVI provides a default gateway for a VLAN.
D. Multiple SVIs can be associated with a VLAN.
E. SVI is another name for a routed port.

Answer: B, C

Explanation: By default all switch ports belongs to VLAN 1 also called switched virtual interface, which is use for switch administration from remote. We can assign the IP address on Virtual Interface so that will be the gateway for VLAN.

QUESTION 436:

Which of the following could be used to provide a Layer 3 data path between separate VLANs? (Choose two.)

A. VLAN trunking
B. An external router
C. An internal route processor
D. VLAN capable bridge
E. EtherChannel

Answer: B, C

Explanation:
To transport packets between VLANs, you must use a Layer 3 device. Traditionally, this has been a
router'sfunction. The router must have a physical or logical connection to each VLAN so that it can
forwardpackets between them. This is known as interVLAN routing.
InterVLANrouting can be performed by an external router that connects to each of the VLANs on
aswitch. Separate physical connections can be used, or the router can access each of the VLANs
througha single trunk link.

QUESTION 437:

Exhibit:

```
CertKiller1(config)# spanning-tree mst configuration
CertKiller1(config-mst)# instance 1 vlan 10-20
CertKiller1(config-mst)# name test
CertKiller1(config-mst)# revision 1
CertKiller1(config-mst)# exit
```

```
CertKiller2(config)# spanning-tree mst configuration
CertKiller2(config-mst)# instance 1 vlan 10-20
CertKiller2(config-mst)# name test
CertKiller2(config-mst)# revision 2
CertKiller2(config-mst)# exit
```

Refer to the show spanning-tree mst configuration output shown in the exhibit.
What should be changed in the configuration of the switch Certkiller 2 in order for it to participate in the same MST region?

A. Switch Certkiller 2 must be configured with a different VLAN range.
B. Switch Certkiller 2 must be configured with a different MST name.
C. Switch Certkiller 2 must be configured with the revision number of 1.
D. Switch Certkiller 2 must be configured with the revision number of 2.

Answer: C

Explanation:
MST is built on the concept of mapping one or more VLANs to a single STP instance. Multiple
instancesof STP can be used (hence the name MST), with each instance supporting a different
groupof VLANs.
In most networks, a single MST region is sufficient, although you can configure more than one

region. Within the region, all switches must run the instance of MST that is defined by the following
attributes:
MST configuration name (32 characters)
MST configuration revision number (0 to 65535)
MST instance-to-VLAN mapping table (4096 entries)
Example of configuration of MST
Switch(config)# spanning-tree mode mst
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name name
Switch(config-mst)# revision version
The configuration revision number gives you a means to track changes to the MST region configuration.Each time you make changes to the configuration, youshould increase the number by one. Remember that the region configuration (including the revision number) must match on all switches in the region. Therefore, you also need to update the revision numbers on the other switchesto match.
Switch(config-mst)# instance instance-id vlan vlan-list
The instance-id (0 to 15) carries topology information for the VLANs listed invlan-list. The list can contain one or more VLANs separated by commas. You can also add a range of VLANs to the list by separating numbers with a hyphen. VLAN numbers can range from 1 to 4094. (Remember that by default, all VLANs are mapped to instance 0, the IST.)
Switch(config-mst)# show pending
regionconfiguration:
Switch(config-mst)# exit
So belong the routers in same MST region, MST attributes should be same, in Certkiller 2 router revision number is not same so to make belong the Certkiller 2 router on same MST region, revision number should be 1.

QUESTION 438:

The network administrator maps VLAN 10 through 20 to MST instance 2. How will this information be propagated to all appropriate switches?

A. Information will be carried in the RSTP BPDUs.
B. It will be propagated in VTP updates.
C. Information stored in the Forwarding Information Base and the switch will reply on query.
D. Multiple Spanning Tree must be manually configured on the appropriate switches.

Answer: D

Explanation:
Recall that the whole idea behind MST is the capability to map multiple VLANs to a smaller number

ofSTP instances. Inside a region, the actual MST instances (MSTIs) exist alongside the IST. Cisco
supportsa maximum of 16 MSTIs in each region. IST always exists as MSTI number 0, leaving
MSTI 1 through 15 available for use.MST must be manually configured on the all switch belongs to same MST region.

QUESTION 439:

Which technology manages multicast traffic at Layer 2 by configuring Layer 2 LAN interfaces dynamically to forward multicast traffic only to those interfaces that want to receive it?

A. IGMP
B. IGMP snooping
C. PIM-DM
D. DVMRP
E. MOSPF

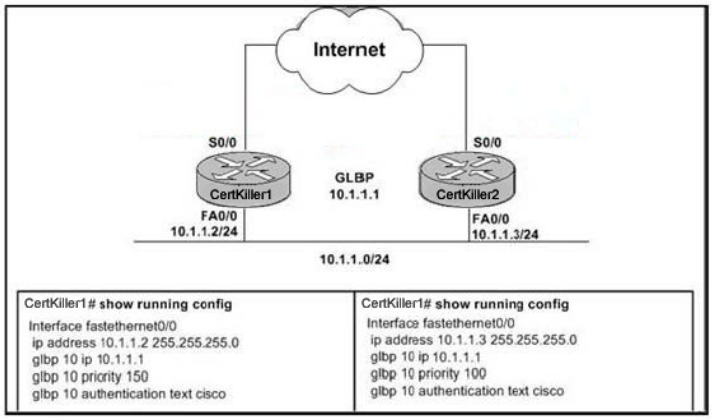
Answer: B

Explanation:
IGMP Snooping
In normal operation, a host desiring multicast group membership must contact a local router so that
itgets added into the multicast tree. IGMP snooping allows a switch to eavesdrop on these IGMP
membershipreports, so that it can find out who is requesting which group.
Recall that to join a group, a host must send its IGMP membership report to the multicast address
ofthe group itself. A Layer 2-only switch must listen to every multicast frame to find the IGMP
information. Clearly, this becomes a burden to the switch CPU.
A multilayer or Layer 3 switch has a clear advantage-it can inherently pick out Layer 3 information
withinframes. This type of switch must listen only to every IGMP packet. When a membership
reportis overheard, the switch adds the multicast group's MAC address to its Content Addressable
Memory (CAM) table (if it doesn't already exist), along with the source switch port where the IGMP
packetwas received. This links the group address with the host who requested membership.
As other hosts request membership to the group, the respective switch ports are added to the CAM
tablelist for the group address. Now, when a frame destined for the multicast group

arrives, it can
bereplicated out exactly the right ports to reach the recipients.

QUESTION 440:

Exhibit:



Refer to the exhibit. Which GLBP device hosts the virtual MAC addresses?

A. R1
B. R2
C. AVG
D. AVF

Answer: D

Explanation:
Active Virtual Gateway
The trick behind this load balancing lies in the GLBP group. One router is elected the active virtual gateway(AVG). This router has the highest priority value, or the highest IP address in the group, if thereis no highest priority. The AVG answers all ARP requests for the virtual router address. Which MAC address it returns depends upon which load-balancing algorithm it is configured to use. In any event, the virtual MAC address supported by one of the routers in the group is returned.
The AVG also assigns the necessary virtual MAC addresses to each of the routers participating in theGLBP group. Up to four virtual MAC addresses can be used in any group. Each of these routers isreferred to as an active virtual forwarder (AVF), forwarding traffic received on its virtual MAC address. Other routers in the group serve as backup or secondary virtual forwarders, in case the AVF
fails. The AVG also assigns secondary roles.
Assign the GLBP priority to a router with the following interface configuration command:
Switch(config-if)# glbp group priority level
GLBP group numbers range from 0 to 1023. The router priority can be 1 to 255 (255 is the highest priority), defaulting to 100.
Active Virtual Forwarder
GLBP uses a weighting function to determine which router becomes the AVF for a virtual MAC addressin a group. Each router begins with a maximum weight value (1 to 254). As specific

interfaces
godown, the weight is decreased by a configured amount. GLBP uses thresholds to determine whena router can and cannot be the AVF. If the weight falls below the lower threshold, the router mustgive up its AVF role. When the weight rises above the upper threshold, the router can resume itsAVF role.
By default, a router receives a maximum weight of 100. If you want to make a dynamic weighting adjustment, GLBP must know which interfaces to track and how to adjust the weight. You must first
definean interface as a tracked object with the following global configuration command:
Switch(config)# track object-number interface type mod/num {line-protocol | iprouting}

QUESTION 441:

Which statement describes the term "multilayer switching"?

A. switches that operate at the access, distribution, and core layer of the design model
B. an OSI Layer 1 and 2 bridging technique
C. a technique to provide hardware switching of Layer 3 unicast packets
D. a flow-based Layer 3 packet routing methodology

Answer: C

Explanation: The device involved in MLS (Multilayer Switching) perform the following functions:
1. Packets are forwarded in hardware that combines Layer 2, Layer 3, and Layer 4 switching.
2. Packets are forwarded at wire speed.
3. The traditional Layer 3 routing function is provided using Cisco Express Forwarding (CEF), wherea database of routes to every destination network is maintained and distributed to switchingASICs for very high forwarding performance.

QUESTION 442:

Which action could have caused the following output to appear on a switch?
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-consistent state

A. The switch is configured with Loop Guard and stops receiving BPDUs.
B. The switch is configured with Port Fast and starts receiving BPDUs.
C. The switch is configured with Root Guard and starts receiving superios BPDUs.
D. The switch is configured with BackboneFast and starts receiving inferior BPDUs.

Answer: C

Explanation:
The root guard feature was developed as a means to control where candidate Root Bridges can be

connectedand found on a network. Basically, a switch learns the cureent Root Bridge's Bridge ID. If another switch advertises a superior BPDU, or one with a better Bridge ID, on a port where root guardis enabled, the local switch will not allow the new switch to become the Root. As long as the superiorBPDUs are being received on the port, the port will be kept in the root-inconsistent STP state. No data can be sent or received in that state, but the switch can listen to BPDUs received on theport.
The following message is printed once root guard blocks a port.
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77. Moved to root-inconsistent state

---

QUESTION 443:

Exhibit:

```
CertKiller# debug ip mrouting 224.2.0.1
MRT: Create (*, 224.2.0.1), if_input NULL
MRT: Create (224.69.15.0/24, 225.2.2.4), if_input Ethernet0, RPF nbr 224.69.61.15
MRT: Create (224.69.39.0/24, 225.2.2.4), if_input Ethernet1, RPF nbr 224.0.0.0
MRT: Create (10.9.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0
MRT: Create (10.16.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0
```

Refer to the exhibit. Given the output of a debug ip mrouting command, which two statements are true? (Choose two.)

A. This router received an IGMP host report from a group member or a PIM join message.
B. The reverse path forwarding (RPF) for the route 224.2.0.1 failed to find the interface on which the multicast packet was received.
C. Multicast route to 10.16.0.0/16 was added to the mroute table and created by a source directly connected to the router.
D. Multicast route to 224.69.15.0/24 was added to the mroute table and created by a source directly connected to the router.
E. The route to 224.69.15.0/24 will be out Ethernet 0.

Answer: A, C

Explanation: Go through this example
debugip mroutingUse the debug ip mrouting EXEC command to display changes to the IP multicast routing table. The no form of this command disables debugging output.
[no] debug ip mrouting [group]
This command tells when the router has made changes to the mroute table. Use the debug ip pim and debug ip mrouting commands at the same time to obtain additional multicast routing information. In addition, use the debug ip igmp command to see why an mroute message is being displayed.
This command generates a large amount of output. Use the optional group to limit the output to a single multicast group.

Sample Display
Router# debugip mrouting 224.2.0.1
MRT: Delete (10.0.0.0/8, 224.2.0.1)MRT: Delete (10.4.0.0/16, 224.2.0.1)MRT: Delete (10.6.0.0/16, 224.2.0.1)MRT: Delete (10.9.0.0/16, 224.2.0.1)MRT: Delete (10.16.0.0/16, 224.2.0.1)MRT: Create (*, 224.2.0.1), if_input NULLMRT: Create (172.24.15.0/24, 225.2.2.4), if_input Ethernet0, RPF nbr 172.16.61.15MRT: Create (172.24.39.0/24, 225.2.2.4), if_input Ethernet1, RPF nbr 0.0.0.0MRT: Create (10.0.0.0/8, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0MRT: Create (10.4.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0MRT: Create (10.6.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0MRT: Create (10.9.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0MRT: Create (10.16.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0Explanations for individual lines of output from Figure 2-108 follow.
The following lines show that multicast IP routes were deleted from the routing table:
MRT: Delete (10.0.0.0/8, 224.2.0.1)MRT: Delete (10.4.0.0/16, 224.2.0.1)MRT: Delete (10.6.0.0/16, 224.2.0.1)The *,G entry in the following line is always null since it is a *,G. The *,G entries are generally created by receipt of an IGMP host-report from a group member on the directly connected LAN or by a PIM join message (in sparse mode) which this router receives from a router that is sending joins toward the RP. This router will in turn, send a join toward the RP which creates the shared tree (or RP tree).
MRT: Create (*, 224.2.0.1), if_input NULLThe following lines are an example of creating an S,G entry that show a mpacket was received on E0. The second line shows a route being created for a source that is on a directly connected LAN. The RPF means "reverse path forwarding," whereby the router looks up the source address of the multicast packet in the unicast routing table and asks which interface will be used to send a packet to that source.
MRT: Create (172.24.15.0/24, 225.2.2.4), if_input Ethernet0, RPF nbr 172.16.61.15MRT: Create (172.24.39.0/24, 225.2.2.4), if_input Ethernet1, RPF nbr 0.0.0.0The following lines show that multicast IP routes were added to the routing table. Note the 0.0.0.0 as the RPF, which means the route was created by a source that is directly connected to this router.
MRT: Create (10.9.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0MRT: Create (10.16.0.0/16, 224.2.0.1), if_input Ethernet1, RPF nbr 0.0.0.0If the source is not directly connected, the nbr address shown in these lines will be the address of the router that forwarded the packet to this router.
The shortest path tree state maintained in routers consists of source (S), multicast address (G), outgoing interface (OIF), and incoming interface (IIF). The forwarding information is referred to as the multicast forwarding entry for (S,G).
An entry for a shared tree can match packets from any source for its associated group if the packets come through the proper incoming interface as determined by the RPF lookup. Such an entry is denoted as (*,G). A (*,G) entry keeps the same information a (S,G) entry keeps, except that it saves the rendezvous point (RP) address in place of the source address in sparse mode or 0.0.0.0 in dense mode.

QUESTION 444:

Exhibit:

CertKiller# **show ip igmp group 232.1.1.1 derail**

```
Interface:      Ethernet3/2
Group:          232.1.1.1
Uptime:         01:58:28
Group mode:     INCLUDE
Last reporter:  10.0.119.133
CSR Grp Exp:    00:02:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote)
  Source Address   Uptime   v3 Exp   CSR Exp   Fwd  Flags
  171.69.214.1     01:58:28 stopped  00:02:31  Yes  C
```

Refer to the exhibit. Given the detailed output of the show ip igmp groups command, which two statements are true? (Choose two.)

A. The rendezvous point (RP) for group 232.1.1.1 is 172.69.214.1.
B. The source for group 232.1.1.1 is 10.0.119.133.
C. The last host to join the group was 10.0.119.133.
D. There are no members using IGMPv3 for group 232.1.1.1.
E. The IP address for interface Ethernet3/2 is 171.69.214.1.

Answer: C, D

Explanation: Last reporter means, last host join on the group is 10.0.119.133. V3 Exp is stopped so no any members using IGMPv3.

QUESTION 445:

You have to configure an Ethernet trunk to operate in ISL mode between two Cisco switches. Which two are required at each end of the link for the trunk to operate correctly? (Choose two.)

A. an identical VTP mode
B. an identical speed/duplex
C. an identical trunk negotiation parameter
D. an identical trunk encapsulation parameter

Answer: B, D

Explanation: To configure the trunk link using ISL, speed/duplex and trunk encapsulation parameter should be same.

QUESTION 446:

Which two tasks are required to configure PIM for IP multicast routing? (Choose two.)

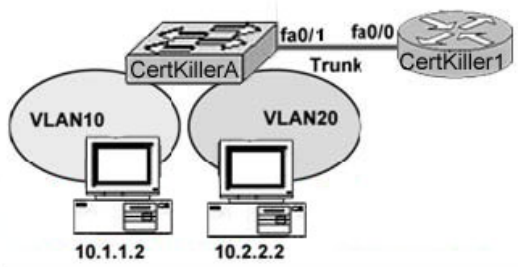
A. Join a multicast group.
B. Enable CGMP.
C. Enable IP multicast routing.
D. Configure the TTL threshold.
E. Enable PIM on an interface.

Answer: C, E

Explanation:
Protocol Independent Multicast (PIM) is a routing protocol that can be used for forwarding multicast
traffic. PIM operates independent of any particular IP routing protocol. Therefore, PIM makes useof the IP unicast routing table and does not keep a separate multicast routing table.
To configure the PIM multicat routing:
i. Enable the multicast routing
switch(Config)# ip multicast-routing
ii. Enable the PIM on an interface
Switch(config-if)# ippim PIM-Mode

QUESTION 447:

Exhibit:




```
CertKiller1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - CSPF inter area
       N1 - OSPF NSSA external type ', N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
    10.1.0.0/24 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0.1
C       10.2.2.0 is directly connected, FastEthernet0/0.2
```

Based on the network diagram and routing table output in the exhibit, which of these statements is true?

A. InterVLAN routing has been configured properly, and the workstations have connectivity to each other.
B. InterVLAN routing will not occur since no routing protocol has been configured.
C. Although interVLAN routing is not enabled, both workstations will have connectivity to each other.
D. Although interVLAN routing is enabled, the workstations will not have connectivity to each other.

Answer: A

Explanation: According to the output of show ip route, InterVLAN routing is configured correctly.

QUESTION 448:

Exhibit:

```
CertKiller1# show run
ip multicast-routing
!
interface Loopback0
ip address 20.0.0.3 255.255.255.255
ip pim sparse-dense-mode
!
interface FastEthernet0/0
ip address 20.0.0.3 255.255.255.255
!
ip pim sparse-dense-mode
ip pim rp-address 1.1.1.1 20
ip pim send-rp-announce Loopback0 scope 32 group-list 10
ip pim send-rp-discovery Loopback0 scope 32
!
access-list 10 permit 224.0.0.0 15.255.255.255
access-list 20 deny 224.0.1.39
access-list 20 deny 224.0.1.40
access-list 20 permit 224.0.0.0 15.255.255.255
```

Study the exhibit. Which statement is true about the configuration?

A. The default rendezvous point for the multicast group 224.0.0.0 is 1.1.1.1.
B. All routers within the 224.0.0.0 group will use 1.1.1.1 as the rendezvous point.
C. All routers within 32 hops will designate address 1.1.1.1 as the rendezvous point for the group.
D. All routers within 32 hops away that are part of group 224.0.0.0 will use 20.0.0.3 as their rendezvous point.

Answer: D

Explanation:
Sparse dense Mode also works on the idea of a shared tree structure, where the root is not

necessarily the
multicastsource. Instead, the root is a PIM-SM router that is centrally located in the network. This rootrouter is called the Rendezvous Point (RP).
According to configuration PIM is enabled in loopback0 interface having address 20.0.0.3 that will be the Rendezvous Point for allowed network 224.0.0.0

QUESTION 449:

Which two attributes must be configured prior to enabling SSH on a Cisco IOS device? (Choose two.)

A. SSH timeout
B. domain name
C. IP address
D. password encryption
E. hostname

Answer: B,E

Explanation: SSH (Secure Shell) is best tool for secure communication, before enabling the ssh you should configured the domain name and hostname.

QUESTION 450:

Which two statements about VTP are correct? (Choose two.)

A. VTP messages will not be forwarded over nontrunk links.
B. VTP domain names need to be identical. However, case doesn't matter.
C. A VTP enabled device which receives multiple advertisements will ignore advertisements with higher configuration revision numbers.
D. A device in "transparent" VTP mode will not forward VTP messages.
E. VTPpruning allows switches to prune VLANs that do not have any active ports associated with them.

Answer: A,E

Explanation: There are two types of link, i. access and ii. trunk link. Access link can carry the information about the only one VLAN and trunk link can carry the information about the more then one VLAN. So, VTP messages will not forwarded over access link.
VTP pruning makes more efficient use of trunk bandwidth by reducing unnecessary flooded traffic. Broadcast and unknown unicast frames on a VLAN are forwarded over a trunk link only if the switchon the receiving end of the trunk has ports in that VLAN. VTP pruning occurs as an extension toVTP version 1, using an additional VTP message type. When a Catalyst switch has a port associated
witha VLAN, the switch sends an advertisement to its neighbor switches that it has active ports

onthat VLAN. The neighbors keep this information, enabling them to decide if flooded traffic from aVLAN should use a trunk port or not.

QUESTION 451:

Which two statements concerning STP state changes are true? (Choose two.)

A. Upon bootup, a port transitions from blocking to forwarding because it assumes itself as root.
B. Upon bootup, a port transitions from blocking to listening because it assumes itself as root.
C. Upon bootup, a port transitions from listening to forwarding because it assumes itself as root.
D. If a forwarding port receives no BPDUs by the max_age time limit, it will transition to listening.
E. If a forwarding port receives an inferior BPDU, it will transition to listening.
F. If a blocked port receives no BPDUs by the max_age time limit, it will transition to listening.

Answer: B,F

Explanation:
When a switch first powers up, it has a narrow view of its surroundings and assumes that it is theRoot Bridge itself. This notion will probably change as other switches check in and enter the electionprocess. The election process then proceeds as follows: Every switch begins by sending out BPDUswith a Root Bridge ID equal to its own Bridge ID and a Sender Bridge ID of its own Bridge ID. The Sender Bridge ID simply tells other switches who is the actual sender of the BPDU message. (After a Root Bridge is decided upon, configuration BPDUs are only sent by the Root Bridge.All other bridges must forward or relay the BPDUs, adding their own Sender Bridge IDs tothe message.)

QUESTION 452:

What will be the effect of applying the VLAN access map configuration on a switch?
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)#action forward
Router(config-access-map)#exit
Router(config)# vlan filter thor vlan-list 12-16

A. All VLAN 12 through 16 IP traffic matching net_10 is forwarded and all other IP packets are dropped.
B. IP traffic matching vlan-list 12-16 is forwarded and all other IP packets are dropped.
C. IP traffic matching net_10 is dropped and all other IP packets are forwarded to VLANs 12 through 16.

D. All VLAN 12 through 16 IP traffic is forwarded, other VLAN IP traffic matching net_10 is dropped.

Answer: A

Explanation:
VACLsare configured as a VLAN access map, in much the same format as a route map. A VLAN accessmap consists of one or more statements, each having a common map name. First, you define theVACL with the following global configuration command:
Switch(config)# vlan access-map map-name [sequence-number]
Access map statements are evaluated in sequence, according to the sequence-number. Each statementcan contain one or more matching conditions, followed by an action.
Next, define the matching conditions that identify the traffic to be filtered. Matching is performed byaccess lists (IP, IPX, or MAC address ACLs), which you must configure independently. Configure amatching condition with the following access map configuration command:
Switch(config-access-map)# match {ip address { acl-number | acl-name}} | {ipx address { acl-number | acl-name}} | {mac address acl-name}
You cane repeat this commmand to define serveral matching conditions ;the first match encountered triggersan action to take. Define the action with the following access map configuration command:
Switch(config-access-map)# action {drop | forward [capture] | redirect interface type mod/num}
A VACL can either drop a matching packet, forward it, or redirect it to another interface. The TCAM performs the entire VACL match and action, as packets are switched or bridged within a VLAN, or routed into or out of a VLAN.
Finally, you must apply the VACL to a VLAN interface using the following global configuration command:
Switch(config)# vlan filter map-name vlan-list vlan-list
Notice that the VACL is applied globally to one or more VLANs listed and not to a VLAN interface (SVI).Recall that VLANs can be present in a switch as explicit interfaces or as inherent Layer 2 entities. The VLAN interface is the point where packets enter or leave a VLAN, so it does not make senseto apply a VACL there. Instead, the VACL needs to function within the VLAN itself, where thereis no inbound or outbound direction.
For example, suppose you find a need to filter traffic within VLAN 99 so that host 192.168.99.17 is notallowed to contact any other host on its local subnet. An access list local-17 is created to identify trafficbetween this host and anything else on its local subnet. Then, a VLAN access map is defined: If the IP address is premitted by the local-17 access list,the packet is dropped;otherwise,it is forwarded. Example 20-1 shows the commands necessary for this example.
Switch1(config)# ip access-list extended local-17
Switch1(config-acl)# permit ip host 192.168.99.17 192.168.99.0 0.0.0.255
Swtich1(config-acl)# exit
Switch1(config)# vlan access-map block-17 10
Switch1(config-access-map)# match ip address local-17
Switch1(config-access-map)# action drop
Switch1(config-access-map)# vlan access-map block-17 20
Switch1(config-access-map)# action forward

Switch1(config-access-map)# exit
Switch1(config)# vlan filter block-17 vlan-list 99

QUESTION 453:

What does the following command accomplish? Switch(config-mst)#instance 10 vlan 11-12

A. enables a PVST+ instance of 10 for vlan 11 and vlan 12
B. enables vlan 11 and vlan 12 to be part of the MST region 10
C. maps vlan 11 and vlan 12 to the MST instance of 10
D. creates an Internal Spanning Tree (IST) instance of 10 for vlan 11 and vlan 12
E. creates a Common Spanning Tree (CST) instance of 10 for vlan 11 and vlan 12
F. starts two instances of MST, one instance for vlan 11 and another instance for vlan 12

Answer: C

Explanation:
MST is built on the concept of mapping one or more VLANs to a single STP instance. Multiple
instancesof STP can be used (hence the name MST), with each instance supporting a different
groupof VLANs.
In most networks, a single MST region is sufficient, although you can configure more than one
region. Within the region, all switches must run the instance of MST that is defined by the following
attributes:
1. MST configuration name (32 characters)
2. MST configuration revision number (0 to 65535)
3. MST instance-to-VLAN mapping table (4096 entries)
Example of configuration of MST
Switch(config)# spanning-tree mode mst
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name name
Switch(config-mst)# revision version
The configuration revision number gives you a means to track changes to the MST region configuration.Each time you make changes to the configuration, youshould increase the number by one. Remember that the region configuration (including the revision number) must match on all switches in the region. Therefore, you also need to update the revision numbers on the other switchesto match.
Switch(config-mst)# instance instance-id vlanvlan-list
The instance-id (0 to 15) carries topology information for the VLANs listed invlan-list. The list can contain one or more VLANs separated by commas.

You can also add a range of VLANs to the list by separating numbers with a hyphen. VLAN numbers can range from 1 to 4094. (Remember that by default, all VLANs are mapped to instance 0, the IST.)
Switch(config-mst)# show pending
regionconfiguration:
Switch(config-mst)# exit

QUESTION 454:

How is the designated querier elected in IGMPv2?

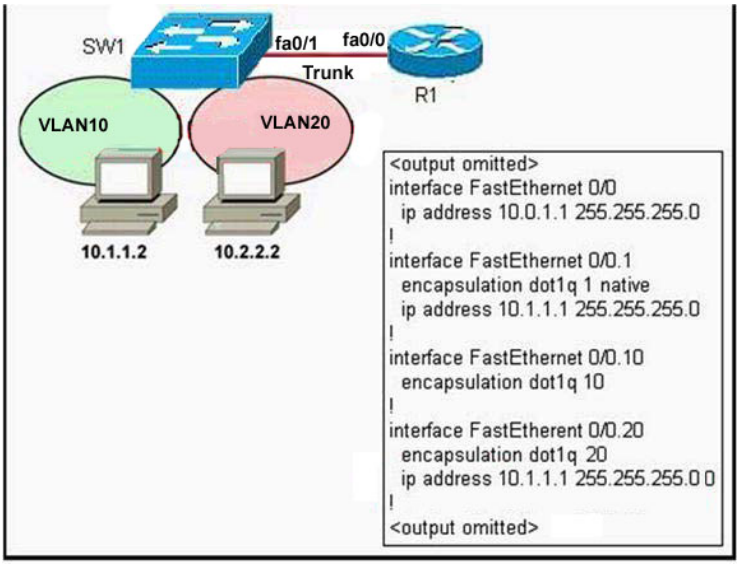
A. The first router to appear on a subnet is designated.
B. The host that responds first to the election query is designated.
C. The router with the lowest IP address on a subnet is designated.
D. The host with the lowest MAC address on a segment is designated.

Answer: C

Explanation: In IGMPv2 designated querier will be the router having lowest IP address on the subnet.

QUESTION 455:

Exhibit:



Refer to the network diagram and partial router configuration shown in the exhibit. What would fix the router configuration and allow packets to be routed between VLANs?

A. Remove the IP address from the physical interface and apply the 10.1.1.1/24 address to the FastEthernet 0/0.10 subinterface.
B. Remove the IP addresses from all subinterfaces.

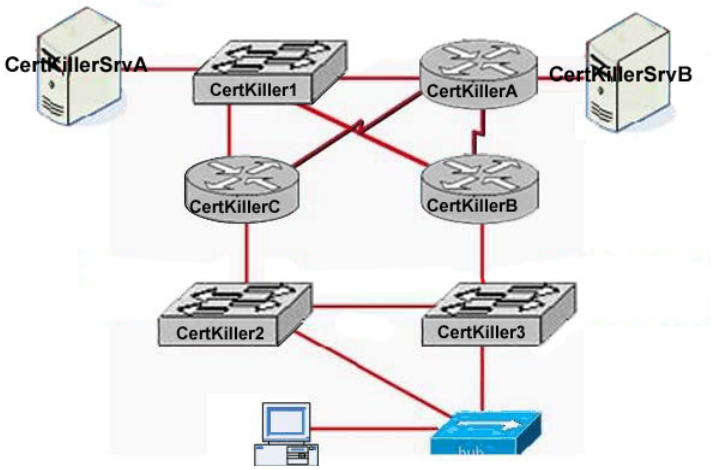
C. Remove the IP address from the physical interface and configure the physical interface for 802.1Q encapsulation.
D. Add a routing protocol to the router so that routing can occur between the VLANs.

Answer: A

Explanation: According output in exhibit, IP Address is assigned in physical interface and one sub-interface. Subinterface is created but IP Address is not assigned.
Assign the IP Address 10.1.1.1 on fa0/0.10 and 10.2.2.1 on fa0/0.20

QUESTION 456:

Exhibit:



Observe the topology in the exhibit. HSRP is configured between Certkiller C and Certkiller B with Certkiller B as the active router. Certkiller 2 is configured as the root bridge for the Spanning Tree Protocol. What will happen if the serial connection on Certkiller B is down?

A. STP will not need to be recalculated because Certkiller C will take over as active router.
B. Certkiller C and Certkiller B will flap between active and standby because the timers for STP are greater than the timers for HSRP.
C. All traffic will automatically forward to Certkiller C.
D. SW3 will take over as the new root bridge.

Answer: B

Explanation: Answer B is correct, Certkiller C and Certkiller B will flap between active and standby because STP has greater time the HSRP.

QUESTION 457:

Which two statements are true about a routed interface on a multilayer switch? (Choose two.)

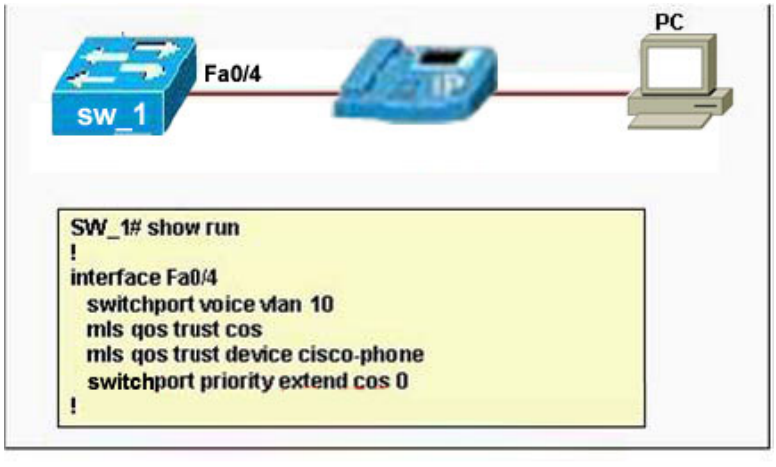
A. A routed port is a virtual switch port on a multilayer switch capable of Layer 3 packet processing.
B. A routed port is created by entering the no switchport command in interface configuration mode.
C. A routed port is associated with a particular VLAN.
D. A routed port can serve as a default gateway for devices that are connected to that port.

Answer: B,D

Explanation:
To verify the configuration of a Layer 2 port, you can use the following EXEC command:
Switch# show interface type mod/num switchport
The output from this command displays the access VLAN or the trunking mode and native VLAN.
The administrative modes reflect what has been configured for the port, while the operational modesshow the port's active status.
See the example:
Switch# show interface fastethernet 0/16 switchport
Name: Fa0/16
Switchport: Disabled
switchportcommand puts the port in Layer 2 mode and no switchport command put the port in Layer 3 mode. Only the Layer 3 port can route the packets between inter VLAN so, Layer 3 port can work as default gateway.

QUESTION 458:

Exhibit:



Refer to the exhibit. A workstation PC is connected to the Cisco IP phone access

port. Based on the configuration in the exhibit, how will the traffic be managed?

A. The IP phone access port will override the priority of the frames received from the PC.
B. The IP phone access port will trust the priority of the frames received from the PC.
C. The switch port Fa0/4 will override the priority of the frames received from the PC.
D. The switch port Fa0/4 will trust the priority for the frames received from the PC.

Answer: A

Explanation:
The PC connected to the phone, however, should normally be untrusted and have all inbound CoS valuesset to 0. This is mentioned here to show how trust boundaries also exist at any connected IP Phones.
Example:
interfacefastethernet 0/1
switchportvoice vlan 200
switchportpriority extend cos 0
A switch instructs an attached IP Phone through CDP messages as to how it should extend QoS trust toits own user data switch port. To configure the trust extension, use the following interface configurationcommand:
Switch(config-if)# switchport priority extend {cos value | trust}
Normally, the QoS information from a PC connected to an IP Phone should not be trusted. This is becausethe PC's applications might try to spoof CoS or Differentiated Services Code Point (DSCP) settingsto gain premium network service. In this case, use the cos keyword so that the CoS bits are overwrittento value by the IP Phone as packets are forwarded to the switch. If CoS values from the PC cannot be trusted, they should be overwritten to a value of 0.

QUESTION 459:

What must be configured on a Cisco switch in order to advertise VLAN information?

A. VTP password
B. VTP domain name
C. VTP revision number
D. VTP mode
E. VTP pruning

Answer: B

Explanation:
VTP is organized into management domains, or areas with common VLAN requirements. A switch canbelong to only one VTP domain, in addition to sharing VLAN information with other switches

inthe domain. Switches in different VTP domains, however, do not share VTP information. Switches in a VTP domain advertise several attributes to their domain neighbors. Each advertisement
containsinformation about the VTP management domain, VTP revision number, known VLANs,and specific VLAN parameters. When a VLAN is added to a switch in a management domain, other switches are notified of the new VLAN through VTP advertisements. In this way, all switchesin a domain can prepare to receive traffic on their trunk ports using the new VLAN.

QUESTION 460:

Exhibit:

```
Switch# show ip def 100.168.150.0
192.168.150.0,24, version 290, cached adjecency 192.168.199.3
0 packets, 0 bytes
via 192.168.199.3, VLAN 199, 0 dependencies
next-hop 192.168.199.3, VLAN 199
valid cached adjacency

Switch# show adjacency detail | begin 192.168.199.3
IP VLAN 199 192.168.199.3(7)
0 packets, 0 bytes
003071006340
.....
...
.
```

Refer to the exhibit. An administrator is verifying that a CEF FIB entry exists to destination network 192.168.150.0. Given the output generated by the show ip cef and show adjacency detail commands, which three statements are true? (Choose three.)

A. There is a valid CEF entry for the destination network 192.168.150.0.
B. The "valid cached adjacency" entry indicates that CEF will put all packets going to such an adjacency to the next best switching mode.
C. The counters (0 packets, 0 bytes) indicate a problem with the 192.168.199.3 next hop IP address.
D. There is an adjacency for the 192.168.199.3 next hop IP address.
E. The number 003071506800 is the MAC address of the 192.168.199.3 next hop IP address.
F. The number 003071506800 is the MAC address of the source IP address.

Answer: A,D,E

QUESTION 461:

What does the command vlan filter accounting_out vlan_list 20 accomplish?

A. specifies the sequence number of 20 for the VLAN map named accounting_out
B. filters all traffic coming into VLAN 20
C. filters traffic specified in access-list 20 on the accounting_out vlan

D. filters traffic specified in accounting_out on VLAN 20

Answer: D

Explanation:
VACLsare configured as a VLAN access map, in much the same format as a route map. A VLAN accessmap consists of one or more statements, each having a common map name. First, you define theVACL with the following global configuration command:
Switch(config)# vlan access-map map-name [sequence-number]
Access map statements are evaluated in sequence, according to the sequence-number. Each statementcan contain one or more matching conditions, followed by an action.
Next, define the matching conditions that identify the traffic to be filtered. Matching is performed byaccess lists (IP, IPX, or MAC address ACLs), which you must configure independently. Configure amatching condition with the following access map configuration command:
Switch(config-access-map)# match {ip address { acl-number | acl-name}} | {ipx address { acl-number | acl-name}} | {mac address acl-name}
You cane repeat this commmand to define serveral matching conditions ;the first match encountered triggersan action to take. Define the action with the following access map configuration command:
Switch(config-access-map)# action {drop | forward [capture] | redirect interface type mod/num}
A VACL can either drop a matching packet, forward it, or redirect it to another interface. The TCAM performs the entire VACL match and action, as packets are switched or bridged within a VLAN, or routed into or out of a VLAN.
Finally, you must apply the VACL to a VLAN interface using the following global configuration command:
Switch(config)# vlan filter map-name vlan-list vlan-list
Notice that the VACL is applied globally to one or more VLANs listed and not to a VLAN interface (SVI).Recall that VLANs can be present in a switch as explicit interfaces or as inherent Layer 2 entities. The VLAN interface is the point where packets enter or leave a VLAN, so it does not make senseto apply a VACL there. Instead, the VACL needs to function within the VLAN itself, where thereis no inbound or outbound direction.
For example, suppose you find a need to filter traffic within VLAN 99 so that host 192.168.99.17 is notallowed to contact any other host on its local subnet. An access list local-17 is created to identify trafficbetween this host and anything else on its local subnet. Then, a VLAN access map is defined: If the IP address is premitted by the local-17 access list,the packet is dropped;otherwise,it is forwarded. Example 20-1 shows the commands necessary for this example.
Switch1(config)# ip access-list extended local-17
Switch1(config-acl)# permit ip host 192.168.99.17 192.168.99.0 0.0.0.255
Swtich1(config-acl)# exit
Switch1(config)# vlan access-map block-17 10
Switch1(config-access-map)# match ip address local-17
Switch1(config-access-map)# action drop
Switch1(config-access-map)# vlan access-map block-17 20
Switch1(config-access-map)# action forward
Switch1(config-access-map)# exit
Switch1(config)# vlan filter block-17 vlan-list 99

QUESTION 462:

What is the purpose of a rendezvous point (RP)?

A. acts as a meeting place for sources and receivers of multicast traffic
B. used in PIM dense mode to create a database of all multicast sources
C. used in PIM dense and sparse mode to create a database of all multicast sources
D. acts as the designated router for a broadcast segment when multicast routing is enabled

Answer: A

Explanation:
Sparse Mode also works on the idea of a shared tree structure, where the root is not necessarily the multicastsource. Instead, the root is a PIM-SM router that is centrally located in the network. This rootrouter is called the Rendezvous Point (RP).

QUESTION 463:

SIMULATION
Exhibit: *** MISSING***
The Certkiller .com headquarter office is installing a temporary Catalyst 3550 in IDF to connect 24 additional users. To prevent network corruption, it is important to have the correct configuration prior to connecting to the production network. It will be necessary to ensure the switch does not participate in VTP but forwards VTP advertisements received on trunk ports.
All interfaces should transition immediately to the forwarding state of Spanning-Tree due to errors that have been experienced on office computers. Also configure the user ports (All FastEthernet ports) so that the ports are permanently non-trunking.

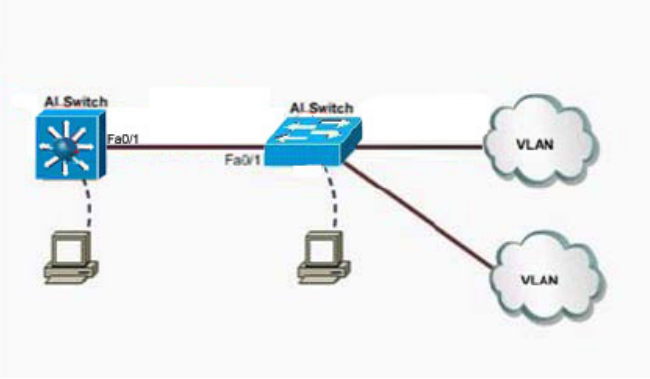
Answer:

Explanation:
Click on Certkiller A
en (Enable Mode)
Enter Password
sh run (See if vlan 20 exists)
config t (Global Config Mode)
vtp mode transparent (Switch does not participate in VTP but forwards VTP advertisements)
vlan 20 (Add vlan if it does not exist)
int range fa0/1 - 24 (Enter range of interface)
spanning-tree portfast (Enable portfast on interfaces)
switchport mode access (Set ports to non-trunking)
exit (Back to Global Config Mode)

int range fa0/12 - 24 (Enter range of interface)
switchport access vlan 20 (Add ports to Vlan 20)
end
sh run (See if config is OK)
copy run start (Save Config)
Short version:
switch#configure terminal
switch(config)#vtp mode transparent
switch(config)#interace range fe0/1 - 24
switch(config-if-range)#switchport mode access
switch(config-if-range)#spanning-tree portfast
switch(config)-if-range#end
switch#copy running-config startup-config
PortFast
An end-user workstation is usually connected to a switch port in the access layer. If the workstation ispowered off and then turned on, the switch port will not be in a usable state until STP cycles from theBlocking state to the Forwarding state. With the default STP timers, this transition takes at least 30 seconds (15 seconds Listening to Learning and 15 seconds Learning to Fowarding). Therefore, theworkstation is unable to transmit or receive any useful data until the Forwarding state is reached onthe port.
According to question, all port should be in non-trunking mode:
Switch(config)# interface range fe0/1 - 24
Switch(config-if)#switchport mode access
Switch(config-if)#spanning-tree portfast : portfast brings the interface in forwarding state.
Switch(config-if)#exit

QUESTION 464:

SIMULATION
Exhibit:



The central offices for a footwear distributor is enhancing their wiring closets with Layer 3 switches. The new distribution layer switch has been installed and a new access layer switch cabled to it. Your task is to configure the distribution layer and access layer switch with VTP to share VLAN information. Then, it is necessary to configure inter-VLAN routing on the distribution layer switch to route traffic between the different VLANs that are configured on the access layer switches.

Specific VLANs and VTP configurations are to be completed in the global configuration mode because VLAN database mode is being deprecated by Cisco. Please reference the following table for the VTP and VLAn information to be configured.
Exhibit #2: *** MISSING ***

Answer:
Click on DLS Switch
en (Enable Mode)
Enter Password
sh run (See ifVlan's exist and Trunking)
config t (Global Config Mode)
vtp mode server (Change vtp mode to server)
vtp domain Distribution (Set VTP Domain)
vlan 20 (Add vlan 20)
vlan 31 (Add vlan 31)
int vlan 20 (Enter interface vlan 20)
ip address 172.16.71.1 255.255.255.0 (Set IP Address of Interface)
no shut (Bring up Interface)
int vlan 31 (Enter interface vlan 31)
ip address 172.16.132.1 255.255.255.0 (Set IP Address of Interface)
no shut (Bring up interface)
exit (Exit from int mode back to Global Config Mode)
ip routing (Enable routing for inter-vlan routing)
Next Set could be optional
int fa0/1 (Enter Ethernet Fa0/1)
switchport trunk encapsulation dotq (Set trunk for 802.1q encapsulation)
switchport mode trunk (Set interface as a trunk)
end
sh run (see if config is OK)
copy run start
Click on ALS Switch
en (Enable Mode)
Enter Password
config t (Global Config Mode)
vtp modeclient (Change vtp mode to server)
vtp domain Distribution (Set VTP Domain)
int fa0/1 (Enter Ethernet Fa0/1)
switchport trunk encapsulation dotq (Set trunk for 802.1q encapsulation)
switchport mode trunk (Set interface as a trunk)
end
sh run (see if config is OK and VLAN 20 and 31 exist in switch config)
copy run start

Explanation:
Identify that the VLAN already exists or not using show run command. DSL switch

should be in VTP server mode, vlan database command is deprecated by cisco so you should do in global configuration mode.
Vtpmode server
Vtpdomain distribution (Setting the VTP domain name).
If VLAN 20 and 31 doesn't exists create it. For InterVLAN routing, assign the IP address on Switched Virtual Interface (VLAN 20 and VLAN 31).
Example: int vlan 20
ip address ipadd netmask
no shutdown
Now You have to enable routing between vlan 20 and 31 using ip routing command
Trunk link can carry the information of multiple VLAN. To configure the trunk link :
Switch(config-if)#switchport trunk encapsulation encapsulation type
Switch(config-if)#switchport mode trunk
In ASL Switch you need to configure the VTP client and one trunk link,
vtpmode client
vtpdomain distribution