Exam : 642-811

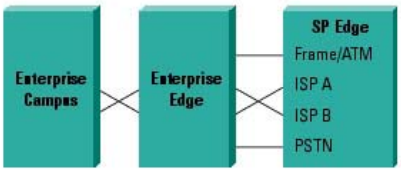
Title : Building Cisco® Multilayer Switched Networks

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_paper09186a008009c8b6.sh

---

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:

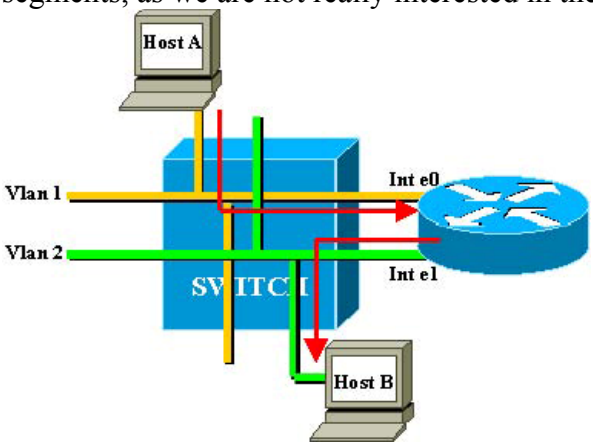
1000BASE-T EIA/TIA Category 5 UTP 4 100 m
1000BASE-SX Multimode fiber (MMF) with 62.5 micron core; 850 nm laser 1
275 m
MMF with 50 micron core; 850 nm laser 1 550 m
1000BASE-LX/LH MMF with 62.5 micron core; 1300 laser 1 550 m
Signal-mode fiber (SMF) with 50 micron core;
1300 nm laser
1 550 m
B: 1000BaseT 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.

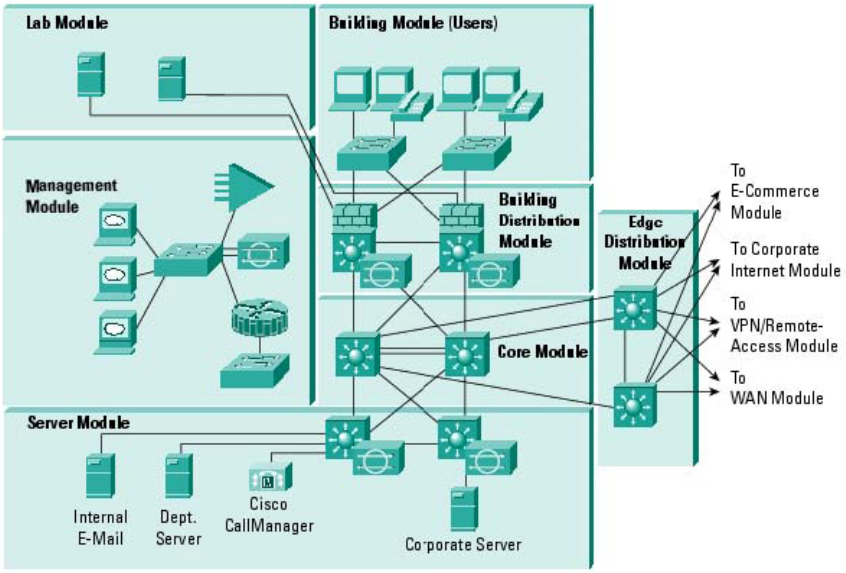
Answer: A, B

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_chapter09186a0080160a7e.htm

---

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_chapter09186a008007fa06.htm

---

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)

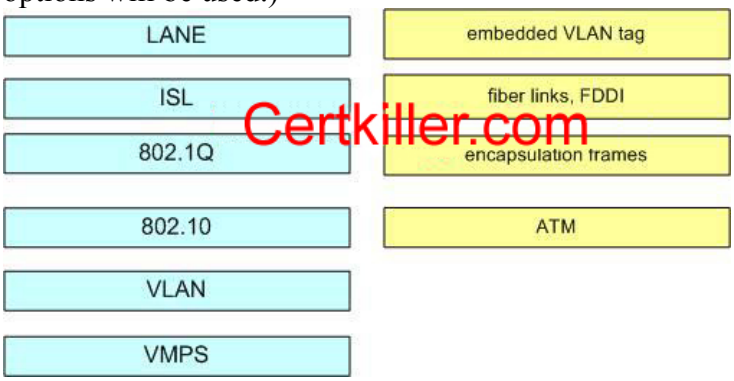
A. An identical VTP mode.
B. An identical speed/duplex.
C. An identical trunk negotiation parameter.
D. An identical trunk encapsulation parameter.

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-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.
