Number: 300-115
Passing Score: 800
Time Limit: 120 min
File Version: 10.0

300-115

Implementing Cisco IP Switched Networks

Version 10.0

Sections

1. Layer 2 Technologies
2. Infrastructure Security
3. Infrastructure Services
4. Mix QUESTIONS

Exam A

QUESTION 1
What is the maximum number of switches that can be stacked using Cisco StackWise?

A. 4
B. 5
C. 8
D. 9
E. 10
F. 13

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Up to 9 Cisco Catalyst switches can be stacked together to build single logical StackWise switch since Cisco IOS XE Release 3.3.0SE. Prior to Cisco IOS XE Release3.3.0SE, up to 4 Cisco Catalyst switches could be stacked together.

Reference: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/qa_c67-722110.html

QUESTION 2
A network engineer wants to add a new switch to an existing switch stack. Which configuration must be added to the new switch before it can be added to the switch stack?

A. No configuration must be added.
B. stack ID
C. IP address
D. VLAN information
E. VTP information

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Switch Stack Offline Configuration

You can use the offline configuration feature to *provision* (to supply a configuration to) a new switch before it joins the switch stack. You can configure in advance the stack member number, the switch type, and the interfaces associated with a switch that is not currently part of the stack. The configuration that you create on the switch stack is called the *provisioned configuration* . The switch that is added to the switch stack and that receives this configuration is called the *provisioned switch*.

You manually create the provisioned configuration through the **switch** *stack-member-number* **provision** *type* global configuration command. The provisioned configuration is automatically created when a switch is added to a switch stack and when no provisioned configuration exists.

When you configure the interfaces associated with a provisioned switch (for example, as part of a VLAN), the switch stack accepts the configuration, and the information appears in the running configuration. The interface associated with the provisioned switch is not active, operates as if it is administratively shut down, and the **no shutdown** interface configuration command does not return it to active service. The interface associated with the provisioned switch does not appear in the display of the specific feature; for example, it does not appear in the **show vlan** user EXEC command output.

The switch stack retains the provisioned configuration in the running configuration whether or not the provisioned switch is part of the stack. You can save the provisioned configuration to the startup configuration file by entering the **copy running-config startup-config** privileged EXEC command. The startup configuration file ensures that the switch stack can reload and can use the saved information whether or not the provisioned switch is part of the switch stack.

Effects of Adding a Provisioned Switch to a Switch Stack

When you add a provisioned switch to the switch stack, the stack applies either the provisioned configuration or the default configuration. Table 5-1 lists the events that occur when the switch stack compares the provisioned configuration with the provisioned switch.

Table 5-1 Results of Comparing the Provisioned Configuration with the Provisioned Switch

Scenario		Result
The stack member numbers and the switch types match.	**1.** If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and **2.** If the switch type of the provisioned switch matches the switch type in the provisioned configuration on the stack.	The switch stack applies the provisioned configuration to the provisioned switch and adds it to the stack.
The stack member numbers match but the switch types do not match.	**1.** If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, but **2.** The switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack.	The switch stack applies the default configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.
The stack member number is not found in the provisioned configuration.		The switch stack applies the default configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.
The stack member number of the provisioned switch is in conflict with an existing stack member.	The stack master assigns a new stack member number to the provisioned switch. The stack member numbers and the switch types match: **1.** If the new stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and **2.** If the switch type of the provisioned switch matches the switch type in the provisioned configuration on the stack.	The switch stack applies the provisioned configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.
	The stack member numbers match, but the switch types do not match: **1.** If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, but **2.** The switch type of the provisioned switch does not match the switch type in the provisioned configuration on the	The switch stack applies the default configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.html

QUESTION 3
What percentage of bandwidth is reduced when a stack cable is broken?

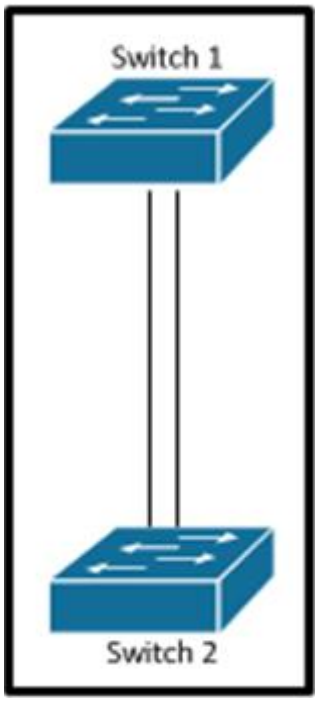
A. 0
B. 25
C. 50
D. 75
E. 100

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Physical Sequential Linkage
The switches are physically connected sequentially, as shown in Figure 3. A break in any one of the cables will result in the stack bandwidth being reduced to half of its full capacity. Subsecond timing mechanisms detect traffic problems and immediately institute failover. This mechanism restores dual path flow when the timing mechanisms detect renewed activity on the cable.
Figure 3. Cisco StackWise Technology Resilient Cabling

Reference: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/prod_white_paper09186a00801b096a.html

QUESTION 4
Refer to the exhibit.



Which set of configurations will result in all ports on both switches successfully bundling into an EtherChannel?

A. switch1
channel-group 1 mode active
switch2
channel-group 1 mode auto

B. switch1
channel-group 1 mode desirable
switch2
channel-group 1 mode passive

C. switch1
channel-group 1 mode on
switch2
channel-group 1 mode auto

D. switch1
channel-group 1 mode desirable
switch2
channel-group 1 mode auto

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The different etherchannel modes are described in the table below:

Mode	Description
active	Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending LACP packets.
auto	Places an interface into a passive negotiating state, in which the interface responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.
desirable	Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending PAgP packets.
on	Forces the interface into an EtherChannel without PAgP or LACP. With the **on** mode, a usable EtherChannel exists only when an interface group in the **on** mode is connected to another interface group in the **on** mode.
passive	Places an interface into a passive negotiating state, in which the interface responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.

Both the auto and desirable PAgP modes allow interfaces to negotiate with partner interfaces to determine if they can form an EtherChannel based on criteria such as interface speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.
Interfaces can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:
- An interface in the desirable mode can form an EtherChannel with another interface that is in the desirable or auto mode.
- An interface in the auto mode can form an EtherChannel with another interface in the desirable mode.

An interface in the auto mode cannot form an EtherChannel with another interface that is also in the auto mode because neither interface starts PAgP negotiation.
An interface in the on mode that is added to a port channel is forced to have the same characteristics as the already existing on mode interfaces in the channel.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swethchl.html

QUESTION 5

Refer to the exhibit.

```
interface GigabitEthernet0/1
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 1-100
!
interface GigabitEthernet0/48
 switchport
 switchport mode access
!
monitor session 1 source interface GigabitEthernet0/1
monitor session 1 destination interface GigabitEthernet0/48
```

How can the traffic that is mirrored out the GigabitEthernet0/48 port be limited to only traffic that is received or transmitted in VLAN 10 on the GigabitEthernet0/1 port?

A. Change the configuration for GigabitEthernet0/48 so that it is a member of VLAN 10.
B. Add an access list to GigabitEthernet0/48 to filter out traffic that is not in VLAN 10.
C. Apply the monitor session filter globally to allow only traffic from VLAN 10.
D. Change the monitor session source to VLAN 10 instead of the physical interface.

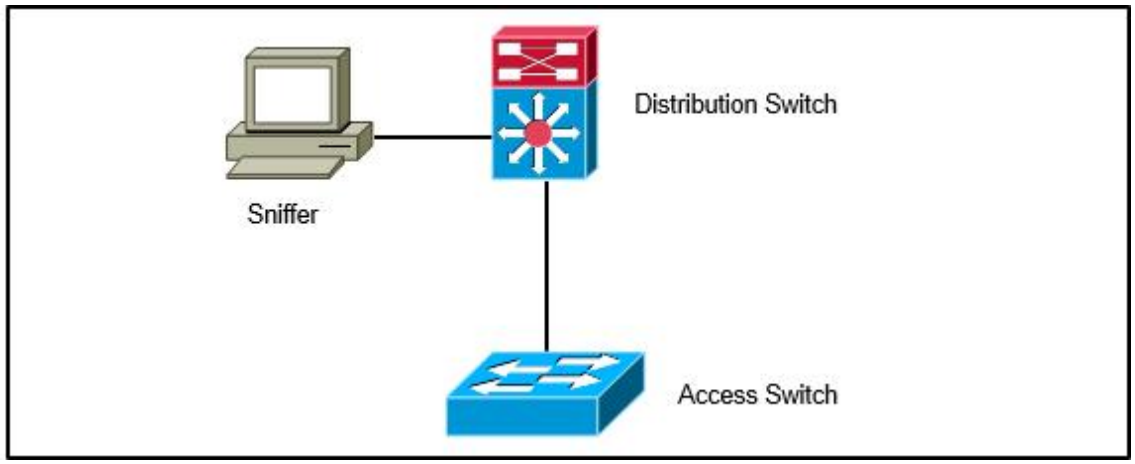
Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the monitor session filter global configuration command.
Usage Guidelines
You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.
You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [, | -] options. If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (-).
VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the monitor session session_number filter vlan vlan-id command to limit SPAN traffic on trunk source ports to only the specified

VLANs.
VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/network_management/command_reference/b_nm_3se_3850_cr/b_nm_3se_3850_cr_chapter_010.html#wp3875419997

QUESTION 6
Refer to the exhibit.



A network engineer wants to analyze all incoming and outgoing packets for an interface that is connected to an access switch. Which three items must be configured to mirror traffic to a packet sniffer that is connected to the distribution switch? (Choose three.)

A. A monitor session on the distribution switch with a physical interface as the source and the remote SPAN VLAN as the destination
B. A remote SPAN VLAN on the distribution and access layer switch
C. A monitor session on the access switch with a physical interface source and the remote SPAN VLAN as the destination
D. A monitor session on the distribution switch with a remote SPAN VLAN as the source and physical interface as the destination
E. A monitor session on the access switch with a remote SPAN VLAN source and the physical interface as the destination
F. A monitor session on the distribution switch with a physical interface as the source and a physical interface as the destination

Correct Answer: BCD
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis.
RSPAN supports source ports, source VLANs, and destination ports on different switches (or different switch stacks), enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html

QUESTION 7
After an EtherChannel is configured between two Cisco switches, interface port channel 1 is in the down/down state. Switch A is configured with channel-group 1 mode active, while Switch B is configured with channel-group 1 mode desirable. Why is the EtherChannel bundle not working?

A. The switches are using mismatched EtherChannel negotiation modes.
B. The switch ports are not configured in trunking mode.
C. LACP priority must be configured on both switches.
D. The channel group identifier must be different for Switch A and Switch B.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Here we have a situation where one switch is using active mode, which is an LACP mode, and the other is using desirable, which is a PAGP mode. You can not mix the LACP and PAGP protocols to form an etherchannel. Here is a summary of the various etherchannel modes:

EtherChannel PagP Modes

Mode	Description
auto	Places a port into a passive negotiating state, in which the port responds to PagP packets it receives but does not start PagP packet negotiation. This setting minimizes the transmission of PagP packets. This mode is not supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel).
Desirable	Places a port into an active negotiating state, in which the port starts negotiations with other ports by sending PagP packets. This mode is not supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel).

EtherChannel LACP Modes

Mode	Description
active	Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
Passive	Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swethchl.html

QUESTION 8
An EtherChannel bundle has been established between a Cisco switch and a corporate web server. The network administrator noticed that only one of the EtherChannel links is being utilized to reach the web server. What should be done on the Cisco switch to allow for better EtherChannel utilization to the corporate web server?

A. Enable Cisco Express Forwarding to allow for more effective traffic sharing over the EtherChannel bundle.
B. Adjust the EtherChannel load-balancing method based on destination IP addresses.
C. Disable spanning tree on all interfaces that are participating in the EtherChannel bundle.
D. Use link-state tracking to allow for improved load balancing of traffic upon link failure to the server.
E. Adjust the EtherChannel load-balancing method based on source IP addresses.

Correct Answer: E
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:

EtherChannel load balancing can use MAC addresses, IP addresses, or Layer 4 port numbers, and either source mode, destination mode, or both. The mode you select applies to all EtherChannels that you configure on the switch. Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel only goes to a single MAC address (which is the case in this example, since all traffic is going to the same web server), use of the destination MAC address results in the choice of the same link in the channel each time. Use of source addresses or IP addresses can result in a better load balance.

Reference: http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html

QUESTION 9
Interface FastEthernet0/1 is configured as a trunk interface that allows all VLANs. This command is configured globally:

monitor session 2 filter vlan 1 – 8, 39, 52

What is the result of the implemented command?

A. All VLAN traffic is sent to the SPAN destination interface.
B. Traffic from VLAN 4 is not sent to the SPAN destination interface.
C. Filtering a trunked SPAN port effectively disables SPAN operations for all VLANs.
D. The trunk's native VLAN must be changed to something other than VLAN 1.
E. Traffic from VLANs 1 to 8, 39, and 52 is replicated to the SPAN destination port.

Correct Answer: E
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The "monitor session filter" command is used to specify which VLANS are to be port mirrored using SPAN. This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the SPAN source is a trunk interface:
Switch(config)# monitor session 2 filter vlan 1 – 5 , 9

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/span.html/index.html#wp1066836

QUESTION 10
A network engineer notices inconsistent Cisco Discovery Protocol neighbors according to the diagram that is provided. The engineer notices only a single neighbor that uses Cisco Discovery Protocol, but it has several routing neighbor relationships. What would cause the output to show only the single neighbor?

A. The routers are connected via a Layer 2 switch.
B. IP routing is disabled on neighboring devices.
C. Cisco Express Forwarding is enabled locally.

D. Cisco Discovery Protocol advertisements are inconsistent between the local and remote devices.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
If all of the routers are connected to each other using a layer 2 switch, then each router will only have the single switch port that it connects to as its neighbor. Even though multiple routing neighbors can be formed over a layer 2 network, only the physical port that it connects to will be seen as a CDP neighbor. CDP can be used to determine the physical topology, but not necessarily the logical topology.

QUESTION 11
After the implementation of several different types of switches from different vendors, a network engineer notices that directly connected devices that use Cisco Discovery Protocol are not visible. Which vendor-neutral protocol could be used to resolve this issue?

A. Local Area Mobility
B. Link Layer Discovery Protocol
C. NetFlow
D. Directed Response Protocol

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP performs functions similar to several proprietary protocols, such as the Cisco Discovery Protocol (CDP).

Reference: http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

QUESTION 12
Several new switches have been added to the existing network as VTP clients. All of the new switches have been configured with the same VTP domain, password, and version. However, VLANs are not passing from the VTP server (existing network) to the VTP clients. What must be done to fix this?

A. Remove the VTP domain name from all switches with "null" and then replace it with the new domain name.
B. Configure a different native VLAN on all new switches that are configured as VTP clients.
C. Provision one of the new switches to be the VTP server and duplicate information from the existing network.

D. Ensure that all switch interconnects are configured as trunks to allow VTP information to be transferred.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP allows switches to advertise VLAN information between other members of the same VTP domain. VTP allows a consistent view of the switched network across all switches. There are several reasons why the VLAN information can fail to be exchanged.
Verify these items if switches that run VTP fail to exchange VLAN information:

- **VTP information only passes through a trunk port. Make sure that all ports that interconnect switches are configured as trunks and are actually trunking.**

Make sure that if EtherChannels are created between two switches, only Layer 2 EtherChannels propagate VLAN information.

- Make sure that the VLANs are active in all the devices.
- One of the switches must be the VTP server in a VTP domain. All VLAN changes must be done on this switch in order to have them propagated to the VTP clients.
- The VTP domain name must match and it is case sensitive. CISCO and cisco are two different domain names.
- Make sure that no password is set between the server and client. If any password is set, make sure that the password is the same on both sides.

Reference: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtml

QUESTION 13
After implementing VTP, the extended VLANs are not being propagated to other VTP switches. What should be configured for extended VLANs?

A. VTP does not support extended VLANs and should be manually added to all switches.
B. Enable VTP version 3, which supports extended VLAN propagation.
C. VTP authentication is required when using extended VLANs because of their ability to cause network instability.
D. Ensure that all switches run the same Cisco IOS version. Extended VLANs will not propagate to different IOS versions when extended VLANs are in use.

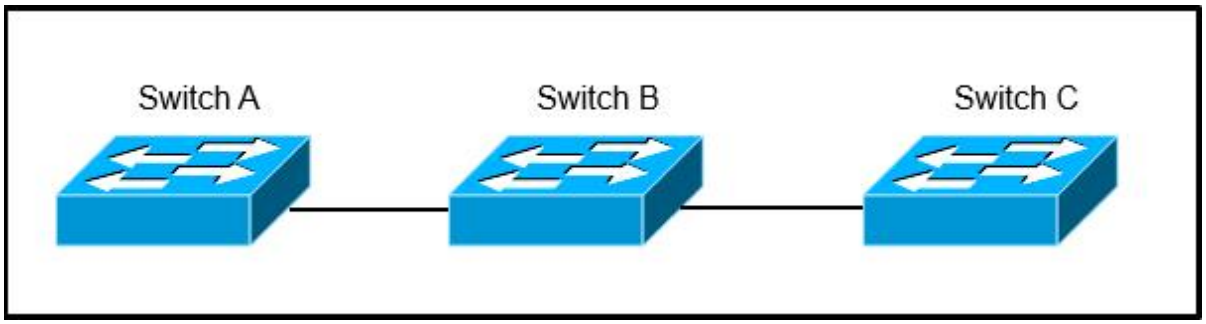
Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:

- VTP version 1 and VTP version 2 do not propagate configuration information for extended-range VLANs (VLAN numbers 1006 to 4094). You must configure extended-range VLANs manually on each network device.
- VTP version 3 supports extended-range VLANs (VLAN numbers 1006 to 4094). If you convert from VTP version 3 to VTP version 2, the VLANs in the range 1006 to 4094 are removed from VTP control.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup2T/vtp.pdf

QUESTION 14
Refer to the exhibit.



Switch A, B, and C are trunked together and have been properly configured for VTP. Switch C receives VLAN information from the VTP server Switch A, but Switch B does not receive any VLAN information. What is the most probable cause of this behavior?

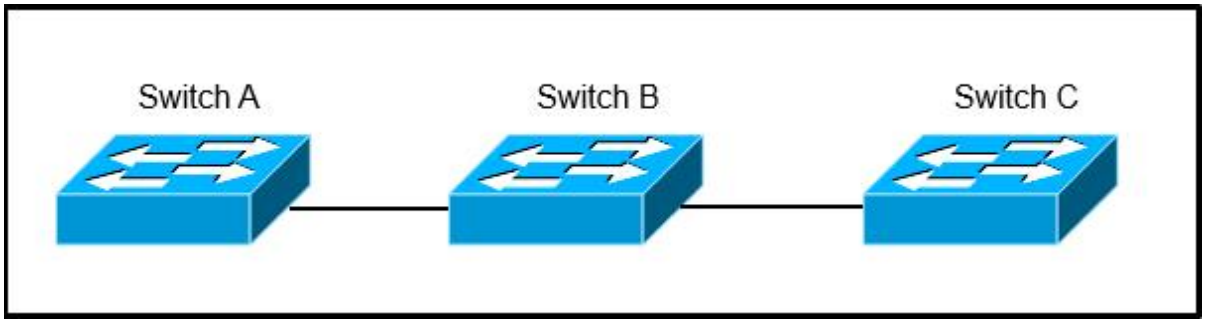
A. Switch B is configured in transparent mode.
B. Switch B is configured with an access port to Switch A, while Switch C is configured with a trunk port to Switch B.
C. The VTP revision number of the Switch B is higher than that of Switch A.
D. The trunk between Switch A and Switch B is misconfigured.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
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, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2.

Reference: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

QUESTION 15
Refer to the exhibit.



Switch A, B, and C are trunked together and have been properly configured for VTP. Switch B has all VLANs, but Switch C is not receiving traffic from certain VLANs. What would cause this issue?

A. A VTP authentication mismatch occurred between Switch A and Switch B.
B. The VTP revision number of Switch B is higher than that of Switch A.
C. VTP pruning is configured globally on all switches and it removed VLANs from the trunk interface that is connected to Switch C.
D. The trunk between Switch A and Switch B is misconfigured.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.
VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. The best explanation for why switch C is not seeing traffic from only some of the VLANs, is that VTP pruning has been configured.

QUESTION 16
After the recent upgrade of the switching infrastructure, the network engineer notices that the port roles that were once “blocking” are now defined as “alternate” and “backup.” What is the reason for this change?

A. The new switches are using RSTP instead of legacy IEEE 802.1D STP.
B. IEEE 802.1D STP and PortFast have been configured by default on all newly implemented Cisco Catalyst switches.
C. The administrator has defined the switch as the root in the STP domain.
D. The port roles have been adjusted based on the interface bandwidth and timers of the new Cisco Catalyst switches.

Correct Answer: A

Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
RSTP works by adding an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge.
RSTP bridge port roles:
* Root port – A forwarding port that is the closest to the root bridge in terms of path cost
* Designated port – A forwarding port for every LAN segment
* Alternate port – A best alternate path to the root bridge. This path is different than using the root port. The alternative port moves to the forwarding state if there is a failure on the designated port for the segment.
* Backup port – A backup/redundant path to a segment where another bridge port already connects. The backup port applies only when a single switch has two links to the same segment (collision domain). To have two links to the same collision domain, the switch must be attached to a hub.
* Disabled port – Not strictly part of STP, a network administrator can manually disable a port

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

QUESTION 17
An administrator recently configured all ports for rapid transition using PortFast. After testing, it has been determined that several ports are not transitioning as they should. What is the reason for this?

A. RSTP has been enabled per interface and not globally.
B. The STP root bridge selection is forcing key ports to remain in non-rapid transitioning mode.
C. STP is unable to achieve rapid transition for trunk links.
D. The switch does not have the processing power to ensure rapid transition for all ports.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
RSTP can only achieve rapid transition to the forwarding state on edge ports and on point-to-point links, not on trunk links. The link type is automatically derived from the duplex mode of a port. A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port by default. This automatic link type setting can be overridden by explicit configuration. In switched networks today, most links operate in full-duplex mode and are treated as point-to-point links by RSTP. This makes them candidates for rapid transition to the forwarding state.

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

QUESTION 18
Which technique automatically limits VLAN traffic to only the switches that require it?

A. access lists
B. DTP in nonegotiate
C. VTP pruning
D. PBR

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets to only the switches that require it. 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 default, VTP pruning is disabled.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vtp.html#wp1020444

QUESTION 19
What effect does the mac address-table aging-time 180 command have on the MAC address-table?

A. This is how long a dynamic MAC address will remain in the CAM table.
B. The MAC address-table will be flushed every 3 minutes.
C. The default timeout period will be 360 seconds.
D. ARP requests will be processed less frequently by the switch.
E. The MAC address-table will hold addresses 180 seconds longer than the default of 10 minutes.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
You can configure the amount of time that an entry (the packet source MAC address and port that packet ingresses) remain in the MAC table.
To configure the aging time for all MAC addresses, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]	Specifies the time before an entry ages out and is discarded from the MAC address table. The range is from 0 to 1000000; the default is 300 seconds. Entering the value 0 disables the MAC aging. If a VLAN is not specified, the aging specification applies to all VLANs.

This example shows how to set the aging time for entries in the MAC address table to 600 seconds (10 minutes):
switch# configure terminal
switch(config)# mac-address-table aging-time 600

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/MACAddress.html#wp1126206

QUESTION 20
While working in the core network building, a technician accidently bumps the fiber connection between two core switches and damages one of the pairs of fiber. As designed, the link was placed into a non-forwarding state due to a fault with UDLD. After the damaged cable was replaced, the link did not recover. What solution allows the network switch to automatically recover from such an issue?

A. macros
B. errdisable autorecovery
C. IP Event Dampening
D. command aliases
E. Bidirectional Forwarding Detection

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
There are a number of events which can disable a link on a Catalyst switch, such as the detection of a loopback, UDLD failure, or a broadcast storm. By

default, manual intervention by an administrator is necessary to restore the interface to working order; this can be done by issuing shutdown followed by no shutdown on the interface. The idea behind requiring administrative action is so that a human engineer can intercede, assess, and (ideally) correct the issue. However, some configurations may be prone to accidental violations, and a steady recurrence of these can amount to a huge time sink for the administrative staff.
This is where errdisable autorecovery can be of great assistance. We can configure the switch to automatically re-enable any error-disabled interfaces after a specified timeout period. This gives the offending issue a chance to be cleared by the user (for example, by removing an unapproved device) without the need for administrative intervention.

Reference: http://packetlife.net/blog/2009/sep/14/errdisable-autorecovery/

QUESTION 21
A network engineer deployed a switch that operates the LAN base feature set and decides to use the SDM VLAN template. The SDM template is causing the CPU of the switch to spike during peak working hours. What is the root cause of this issue?

A. The VLAN receives additional frames from neighboring switches.
B. The SDM VLAN template causes the MAC address-table to overflow.
C. The VLAN template disables routing in hardware.
D. The switch needs to be rebooted before the SDM template takes effect.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
SDM Template Notes:
- All templates are predefined. There is no way to edit template category individual values.
- The switch reload is required to use a new SDM template.
- The ACL merge algorithm, as opposed to the original access control entries (ACEs) configured by the user, generate the number of TCAM entries listed for security and QoS ACEs.
- The first eight lines (up to Security ACEs) represent approximate hardware boundaries set when a template is used. If the boundary is exceeded, all processing overflow is sent to the CPU which can have a major impact on the performance of the switch.

Choosing the VLAN template will actually disable routing (number of entry for unicast or multicast route is zero) in hardware.

Reference: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/44921-swdatabase-3750ss-44921.html

QUESTION 22
An access switch has been configured with an EtherChannel port. After configuring SPAN to monitor this port, the network administrator notices that not all traffic is being replicated to the management server. What is a cause for this issue?

A. VLAN filters are required to ensure traffic mirrors effectively.
B. SPAN encapsulation replication must be enabled to capture EtherChannel destination traffic.

C. The port channel can be used as a SPAN source, but not a destination.
D. RSPAN must be used to capture EtherChannel bidirectional traffic.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

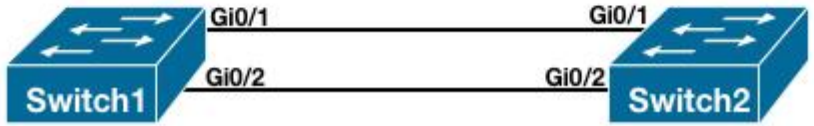
Explanation/Reference:
Explanation:
A source port or EtherChannel is a port or EtherChannel monitored for traffic analysis. You can configure both Layer 2 and Layer 3 ports and EtherChannels as SPAN sources. SPAN can monitor one or more source ports or EtherChannels in a single SPAN session. You can configure ports or EtherChannels in any VLAN as SPAN sources. Trunk ports or EtherChannels can be configured as sources and mixed with nontrunk sources. A port-channel interface (an EtherChannel) can be a SPAN source, but not a destination.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.html#wp1040905

QUESTION 23
Refer to the exhibit.

```
hostname Switch1
<output omitted>
!
port-channel load-balance dst-ip
!
interface GigabitEthernet0/1
 channel-group 10 mode active
!
interface GigabitEthernet0/2
 channel-group 10 mode passive
!
```

```
hostname Switch2
<output omitted>
!
port-channel load-balance src-mac
!
interface GigabitEthernet0/1
 channel-group 10 mode passive
!
interface GigabitEthernet0/2
 channel-group 10 mode active
!
```



What is the result of the configuration?

A. The EtherChannels would not form because the load-balancing method must match on the devices.
B. The EtherChannels would form and function properly even though the load-balancing and EtherChannel modes do not match.
C. The EtherChannels would form, but network loops would occur because the load-balancing methods do not match.
D. The EtherChannels would form and both devices would use the dst-ip load-balancing method because Switch1 is configured with EtherChannel mode active.

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
An etherchannel will form if one end is active and the other is passive. The table below summarizes the results for LACP channel establishment based on the configuration of each side of a link:

LACP Channel Establishment

S1	S2	Established?
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	Not Configured	No
On	Active	No
Passive/On	Passive	No

Load balancing can only be configured globally. As a result, all channels (manually configured, PagP, or LACP) use the same load-balancing. This is true for the switch globally, although each switch involved in the etherchannel can have non matching parameters for load balancing.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/54sg/configuration/guide/config/channel.html#wp1020804

QUESTION 24
A network engineer tries to configure storm control on an EtherChannel bundle. What is the result of the configuration?

A. The storm control settings will appear on the EtherChannel, but not on the associated physical ports.
B. The configuration will be rejected because storm control is not supported for EtherChannel.
C. The storm control configuration will be accepted, but will only be present on the physical interfaces.
D. The settings will be applied to the EtherChannel bundle and all associated physical interfaces.

Correct Answer: D

Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
After you configure an EtherChannel, any configuration that you apply to the port-channel interface affects the EtherChannel; any configuration that you apply to the physical interfaces affects only the interface where you apply the configuration.
Storm Control is an exception to this rule. For example, you cannot configure Storm Control on some of the members of an EtherChannel; Storm Control must be configured on all or none of the ports. If you configure Storm Control on only some of the ports, those ports will be dropped from the EtherChannel interface (put in suspended state). Therefore, you should configure Storm Control at the EtherChannel Interface level, and not at the physical interface level.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/channel.html

QUESTION 25
What is the function of NSF?

A. forward traffic simultaneously using both supervisors
B. forward traffic based on Cisco Express Forwarding
C. provide automatic failover to back up supervisor in VSS mode
D. provide nonstop forwarding in the event of failure of one of the member supervisors

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VSS is network system virtualization technology that pools multiple Cisco Catalyst 6500 Series Switches into one virtual switch, increasing operational efficiency, boosting nonstop communications, and scaling system bandwidth capacity to 1.4 Tbps. Switches would operate as a single logical virtual switch called a virtual switching system 1440 (VSS1440). VSS formed by two Cisco Catalyst 6500 Series Switches with the Virtual Switching Supervisor 720-10GE.
In a VSS, the data plane and switch fabric with capacity of 720 Gbps of supervisor engine in each chassis are active at the same time on both chassis, combining for an active 1400-Gbps switching capacity per VSS. Only one of the virtual switch members has the active control plane. Both chassis are kept in sync with the inter-chassis Stateful Switchover (SSO) mechanism along with Nonstop Forwarding (NSF) to provide nonstop communication even in the event of failure of one of the member supervisor engines or chassis.

Reference: http://ciscorouterswitch.over-blog.com/article-cisco-catalyst-6500-series-vss-1440-124536783.html

QUESTION 26
After UDLD is implemented, a Network Administrator noticed that one port stops receiving UDLD packets. This port continues to reestablish until after eight failed retries. The port then transitions into the errdisable state. Which option describes what causes the port to go into the errdisable state?

A. Normal UDLD operations that prevent traffic loops.
B. UDLD port is configured in aggressive mode.
C. UDLD is enabled globally.
D. UDLD timers are inconsistent.

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/udld.html

QUESTION 27
After reviewing UDLD status on switch ports, an engineer notices that the." Which statement describes what this indicates about the status of the port?

A. The port is fully operational and no known issues are detected.
B. The bidirectional status of "unknown" indicates that the port will go into the disabled state because it stopped receiving UDLD packets from its neighbor.
C. UDLD moved into aggressive mode after inconsistent acknowledgements were detected.
D. The UDLD port is placed in the "unknown" state for 5 seconds until the next UDLD packet is received on the interface.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
By default, UDLD is disabled on all interfaces. We can enable UDLD globally on the device, or individually on specific interfaces with the command udld port. This enables UDLD in normal mode.
It would be prohibitively difficult to coordinate the configuration of UDLD on both ends of a link at the same time, so when UDLD is first enabled and does not detect a neighbor the link state is considered unknown, which is not necessarily an error condition. The port will remain operational during this time. When UDLD is finally enabled on the other end, the status will transition to bidirectional.

Reference: http://packetlife.net/blog/2011/mar/7/udld/

QUESTION 28

Pilot testing of the new switching infrastructure finds that when the root port is lost, STP immediately replaces the root port with an alternative root port. Which spanning-tree technology is used to accomplish backup root port selection?

A. PVST+
B. PortFast
C. BackboneFast
D. UplinkFast
E. Loop Guard
F. UDLD

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
I f a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the spanning-tree uplinkfast global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures.
UplinkFast provides fast convergence after a direct link failure and achieves load balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 interfaces (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, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swstpopt.html

QUESTION 29
A network engineer must adjust the STP interface attributes to influence root port selection. Which two elements are used to accomplish this? (Choose two.)

A. port-priority
B. cost
C. forward-timers
D. link type
E. root guard

Correct Answer: AB
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.
When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstp.html

QUESTION 30
A network engineer must set the load balance method on an existing port channel. Which action must be done to apply a new load balancing method?

A. Configure the new load balancing method using port-channel load-balance.
B. Adjust the switch SDM back to “default”.
C. Ensure that IP CEF is enabled globally to support all load balancing methods.
D. Upgrade the PFC to support the latest load balancing methods.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Example:
EtherChannel balances the traffic load across the links in a channel through the reduction of part of the binary pattern that the addresses in the frame form to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The mode applies to all EtherChannels that are configured on the switch. You configure the load balancing and forwarding method with use of the **port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}** global configuration command.

Reference: http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html

QUESTION 31
Refer to the exhibit.

```
Switch#sh int g0/12
GigabitEthernet0/23 is up, line protocol is down (monitoring)
  Hardware is C6k 1000Mb 802.3, address is 001c.f9d4.7500 (bia
  001c.f9d4.750)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    Reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
```

A network engineer investigates a recent network failure and notices that one of the interfaces on the switch is still down. What is causing the line protocol on this interface to be shown as down?

A. There is a layer 1 physical issue.
B. There is a speed mismatch on the interface.
C. The interface is configured as the target of the SPAN session.
D. The interface is configured as the source of the SPAN session.
E. There is a duplex mismatch on the interface.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
With the SAPN destination port, the state of the destination port is up/down by design. The interface shows the port in this state in order to make it evident that the port is currently not usable as a production port. This is the normal operational state for SPAN destinations.

Reference: http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml

QUESTION 32
While doing network discovery using Cisco Discovery Protocol, it is found that rapid error tracking is not currently enabled. Which option must be enabled to allow for enhanced reporting mechanisms using Cisco Discovery Protocol?

A. Cisco Discovery Protocol version 2
B. Cisco IOS Embedded Event Manager
C. logging buffered

D. Cisco Discovery Protocol source interface
E. Cisco Discovery Protocol logging options

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
- CDP Version 1 — This is the first version of CDP which was used for the discovery of Cisco devices in the network. This version is mainly used for backward compatibility.
- CDP Version 2 — This is the most recent version of CDP which has enhanced features such as rapid reporting mechanism, which is used to track down errors and minimize costly downtime. It allows you to track instances even if the native VLAN ID or port duplex states do not match between connecting devices. This is the default version on all switches.

Reference: http://sbkb.cisco.com/CiscoSB/GetArticle.aspx?docid=0ed03cbac49b446ab390a657917d817c_Cisco_Discovery_Protocol_CDP__Properties_Settings_on_Sx500_S.xml&pid=2&converted=0

QUESTION 33
Which technique allows specific VLANs to be strictly permitted by the administrator?

A. VTP pruning
B. transparent bridging
C. trunk allowed VLANs
D. VLAN access-list
E. L2P tunneling

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the "switchport trunk allowed vlan remove vlan-list" interface configuration command to remove specific VLANs from the allowed list.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_13_ea1/configuration/guide/swvlan.html

QUESTION 34
For security reasons, the IT manager has prohibited users from dynamically establishing trunks with their associated upstream switch. Which two actions can prevent interface trunking? (Choose two.)

A. Configure trunk and access interfaces manually.
B. Disable DTP on a per interface basis.
C. Apply BPDU guard and BPDU filter.
D. Enable switchport block on access ports.

Correct Answer: AB
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The Dynamic Trunking Protocol (DTP) is used to negotiate forming a trunk between two Cisco devices. DTP causes increased traffic, and is enabled by default, but may be disabled. To disable DTP, configure “switchport nonegotiate.” This 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.

Reference: http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=8

QUESTION 35
Which two protocols can be automatically negotiated between switches for trunking? (Choose two.)

A. PPP
B. DTP
C. ISL
D. HDLC
E. DLCI
F. DOT1Q

Correct Answer: CF
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Switches such as the Catalyst 3550 that are capable of either 802.1Q or ISL trunking encapsulation, the switchport trunk encapsulation [dot1q | isl | negotiate] interface command must be used prior to the switchport mode trunk command.

Reference: https://learningnetwork.cisco.com/servlet/JiveServlet/previewBody/14792-102-1-57313/Dynamic%20Trunking%20Protocol.PDF

QUESTION 36

A network is running VTPv2. After verifying all VTP settings, the network engineer notices that the new switch is not receiving the list of VLANs from the server. Which action resolves this problem?

A. Reload the new switch.
B. Restart the VTP process on the new switch.
C. Reload the VTP server.
D. Verify connected trunk ports.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP should never need to have the switch reloaded or the VTP process to restart in order for it to work. The first thing that should be done is to verify that the trunk ports are connected and up.

QUESTION 37
After configuring new data VLANs 1020 through 1030 on the VTP server, a network engineer notices that none of the VTP clients are receiving the updates. What is the problem?

A. The VTP server must be reloaded.
B. The VTP version number must be set to version 3.
C. After each update to the VTP server, it takes up to 4 hours propagate.
D. VTP must be stopped and restarted on the server.
E. Another switch in the domain has a higher revision number than the server.

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP version 3 supports these features that are not supported in version 1 or version 2:

- Enhanced authentication—You can configure the authentication as hidden or secret. When hidden, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the secret keyword, you can directly configure the password secret key.
- **Support for extended range VLAN (VLANs 1006 to 4094) database propagation. VTP versions 1 and 2 propagate only VLANs 1 to 1005. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2.**

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_52_se/configuration/guide/swvtp.html#wp1316856

QUESTION 38
A network engineer is extending a LAN segment between two geographically separated data centers. Which enhancement to a spanning-tree design prevents unnecessary traffic from crossing the extended LAN segment?

A. Modify the spanning-tree priorities to dictate the traffic flow.
B. Create a Layer 3 transit VLAN to segment the traffic between the sites.
C. Use VTP pruning on the trunk interfaces.
D. Configure manual trunk pruning between the two locations.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Pruning unnecessary VLANs from the trunk can be performed with one of two methods:
- Manual pruning of the unnecessary VLAN on the trunk—This is the best method, and it avoids the use of the spanning tree. Instead, the method runs the pruned VLAN on trunks.
- VTP pruning—Avoid this method if the goal is to reduce the number of STP instances. VTP-pruned VLANs on a trunk are still part of the spanning tree. Therefore, VTP-pruned VLANs do not reduce the number of spanning tree port instances.

Since the question asked for the choice that is an enhancement to the STP design, VTP pruning is the best choice.

Reference: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtml

QUESTION 39
The network manager has requested that several new VLANs (VLAN 10, 20, and 30) are allowed to traverse the switch trunk interface. After the command switchport trunk allowed vlan 10,20,30 is issued, all other existing VLANs no longer pass traffic over the trunk. What is the root cause of the problem?

A. The command effectively removed all other working VLANs and replaced them with the new VLANs.
B. VTP pruning removed all unused VLANs.
C. ISL was unable to encapsulate more than the already permitted VLANs across the trunk.
D. Allowing additional VLANs across the trunk introduced a loop in the network.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:

Explanation:
The “switchport trunk allowed vlan” command will only allow the specified VLANs, and overwrite any others that were previously defined. You would also need to explicitly allow the other working VLANs to this configuration command, or use the “issue the switchport trunk allowed vlan add vlan-list” command instead to add these 3 VLANS to the other defined allowed VLANs.

Reference: https://supportforums.cisco.com/document/11836/how-define-vlans-allowed-trunk-link

QUESTION 40
When you design a switched network using VTPv2, how many VLANs can be used to carry user traffic?

A. 1000
B. 1001
C. 1024
D. 2048
E. 4095
F. 4096

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP versions 1 and 2 Supports normal VLAN numbers (1-1001). Only VTP version 3 supports extended VLANs (1-4095).

Reference: http://cciememo.blogspot.com/2012/11/difference-between-vtp-versions.html

QUESTION 41
What does the command vlan dot1q tag native accomplish when configured under global configuration?

A. All frames within the native VLAN are tagged, except when the native VLAN is set to 1.
B. It allows control traffic to pass using the non-default VLAN.
C. It removes the 4-byte dot1q tag from every frame that traverses the trunk interface(s).
D. Control traffic is tagged.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:

The “vlan dot1q tag native” will tag all untagged frames, including control traffic, with the defined native VLAN.

QUESTION 42
A network engineer has just deployed a non-Cisco device in the network and wants to get information about it from a connected device. Cisco Discovery Protocol is not supported, so the open standard protocol must be configured. Which protocol does the network engineer configure on both devices to accomplish this?

A. IRDP
B. LLDP
C. NDP
D. LLTD

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP performs functions similar to several proprietary protocols, such as the Cisco Discovery Protocol (CDP).

Reference: http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

QUESTION 43
A manager tells the network engineer to permit only certain VLANs across a specific trunk interface. Which option can be configured to accomplish this?

A. allowed VLAN list
B. VTP pruning
C. VACL
D. L2P tunneling

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
When a trunk link is established, all of the configured VLANs are allowed to send and receive traffic across the link. VLANs 1 through 1005 are allowed on each trunk by default. However, VLAN traffic can be removed from the allowed list. This keeps traffic from the VLANs from passing over the trunk link.

Note: The allowed VLAN list on both the ends of the trunk link should be the same.
For Integrated Cisco IOS Software based switches, perform these steps:
1. To restrict the traffic that a trInk carries, issue the switchport trunk vlan-list interface configuration command. This removes specific VLANs from the allowed list.

Reference: https://supportforums.cisco.com/document/11836/how-define-vlans-allowed-trunk-link

QUESTION 44
For client server failover purposes, the application server team has indicated that they must not have the standard 30 second delay before their switchport enters a forwarding state. For their disaster recovery feature to operate successfully, they require the switchport to enter a forwarding state immediately. Which spanning-tree feature satisfies this requirement?

A. Rapid Spanning-Tree
B. Spanning-Tree Timers
C. Spanning-Tree FastPort
D. Spanning-Tree PortFast
E. Spanning-Tree Fast Forward

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
In order to allow immediate transition of the port into forwarding state, enable the STP PortFast feature. PortFast immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.
Example configuration:
Switch-C# configure terminal
Switch-C(config)# interface range fa0/3 - 24
Switch-C(config-if-range)# sp–nning-tree portfast

Reference: http://www.informit.com/library/content.aspx?b=CCNP_Studies_Switching&seqNum=36

QUESTION 45
Which command does a network engineer use to verify the spanning-tree status for VLAN 10?

A. switch# show spanning-tree vlan 10
B. switch# show spanning-tree bridge
C. switch# show spanning-tree brief
D. switch# show spanning-tree summary

E. switch# show spanning-tree vlan 10 brief

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

Example output:
SW2#show spanning-tree vlan 10

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    24586
             Address     0014.f2d2.4180
             Cost        9
             Port        216 (Port-channel21)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     001c.57d8.9000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Po21                Root FWD 9         128.216  P2p
Po23                Altn BLK 9         128.232  P2p
```

Reference: http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_s2.html

QUESTION 46
A new network that consists of several switches has been connected together via trunking interfaces. If all switches currently have the default VTP domain name "null", which statement describes what happens when“a do”ain name is configured on one of the switches?

A. The switch with the non-default domain name restores back to "null" upon reboot.
B. Switches with higher revisio“ num”ers does not accept the new domain name.

C. VTP summary advertisements are sent out of all ports with the new domain name.
D. All other switches with the default domain name become VTP clients.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
By default, a switch will have a domain name of NULL and no password. If the switch hears a VTP advertisement it will automatically learn the VTP domain name, VLANs, and the configuration revision number.
Summary advertisements – sent out every 300 seconds and every time a change occurs on the VLAN database. Contained in a summary advertisement:

- VTP version
- **Domain name**
- Configuration revision number
- Time stamp
- MD5 encryption hash code

Reference: https://rowell.dionicio.net/configuring-cisco-vtp/

QUESTION 47
A network engineer is setting up a new switched network. The network is expected to grow and add many new VLANs in the future. Which Spanning Tree Protocol should be used to reduce switch resources and managerial burdens that are associated with multiple spanning-tree instances?

A. RSTP
B. PVST
C. MST
D. PVST+
E. RPVST+

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Multiple Spanning Tree (MST) extends the IEEE 802.1w RST algorithm to multiple spanning trees. The main purpose of MST is to reduce the total number of spanning-tree instances to match the physical topology of the network and thus reduce the CPU cycles of a switch. PVRST+ runs STP instances for each VLAN and does not take into consideration the physical topology that might not require many different STP topologies. MST, on the other hand, uses a minimum number of STP instances to match the number of physical topologies present.
Figure 3-15 shows a common network design, featuring an access Switch A, connected to two Building Distribution submodule Switches D1 and D2. In

this setup, there are 1000 VLANs, and the network administrator typically seeks to achieve load balancing on the access switch uplinks based on even or odd VLANs—or any other scheme deemed appropriate.

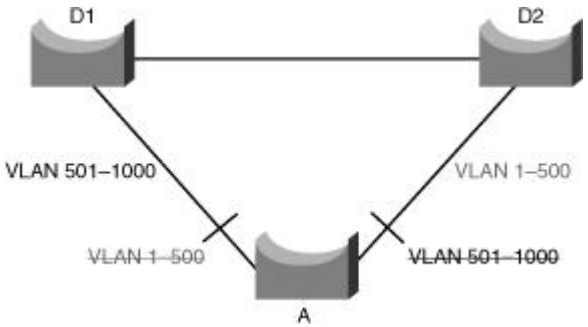


Figure 3-15: VLAN Load Balancing
Figure 3-15 illustrates two links and 1000 VLANs. The 1000 VLANs map to two MST instances. Rather than maintaining 1000 spanning trees, each switch needs to maintain only two spanning trees, reducing the need for switch resources.

Reference: http://ciscodocuments.blogspot.com/2011/05/chapter-03-implementing-spanning-tree_19.html

QUESTION 48
Which statement about the use of SDM templates in a Cisco switch is true?

A. SDM templates are used to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network.
B. SDM templates are used to create Layer 3 interfaces (switch virtual interfaces) to permit hosts in one VLAN to communicate with hosts in another VLAN.
C. SDM templates are used to configure ACLs that protect networks and specific hosts from unnecessary or unwanted traffic.
D. SDM templates are used to configure a set of ACLs that allows the users to manage the flow of traffic handled by the route processor.
E. SDM templates are configured by accessing the switch using the web interface.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
You can use SDM templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can select a template to provide maximum system usage for some functions; for example, use the default template to balance resources, and use access template to obtain maximum ACL usage. To allocate hardware resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_55_se/configuration/guide/swsdm.pdf

QUESTION 49
Which SDM template disables routing and supports the maximum number of unicast MAC addresses?

A. VLAN
B. access
C. default
D. routing

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To allocate ternary content addressable memory (TCAM) resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features. You can select SDM templates to optimize these features:

- Access — The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- Default — The default template gives balance to all functions.
- Routing — The routing template maximizes system resources for Ipv4 unicast routing, typically required for a router or aggregator in the center of a network.
- **VLANs — The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.**

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swsdm.pdf

QUESTION 50
Which SDM template is the most appropriate for a Layer 2 switch that provides connectivity to a large number of clients?

A. VLAN
B. default
C. access
D. routing

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:

Explanation:
To allocate ternary content addressable memory (TCAM) resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features. You can select SDM templates to optimize these features:

- Access—The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- Default—The default template gives balance to all functions.
- Routing—The routing template maximizes system resources for Ipv4 unicast routing, typically required for a router or aggregator in the center of a network.
- **VLANs—The VLAN template disables routing and supports the maximum number of unicast MAC addresses (clients). It would typically be selected for a Layer 2 switch.**

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swsdm.pdf

QUESTION 51
In a Cisco switch, what is the default period of time after which a MAC address ages out and is discarded?

A. 100 seconds
B. 180 seconds
C. 300 seconds
D. 600 seconds

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To configure the aging time for all MAC addresses, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]	Specifies the time before an entry ages out and is discarded from the MAC address table. The range is from 0 to 1000000; **the default is 300 seconds**. Entering the value 0 disables the MAC aging. If a VLAN is not specified, the aging specification applies to all VLANs.

Reference: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/MACAddress.html