Cisco Certified Network Professional (CCNP)

Exam 300-115 Implementing Cisco IP Switched Networks (S I C)

Multiple Choice Questions

CISCO

CISCO CERTIFIED CCNP

(300-115) Implementing Cisco IP Switched Networks

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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

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: part1
Explanation

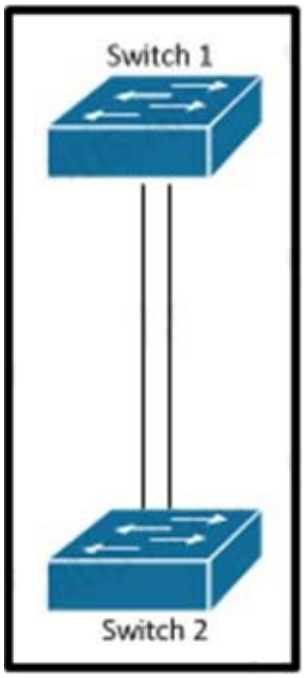
Explanation/Reference:

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: part1
Explanation

Explanation/Reference:
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 re- sponds to PAgP packets it receives but does not start PAgP packet negotia- tion.
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 re- sponds to LACP packets that it receives, but does not start LACP packet ne-gotiation. 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?

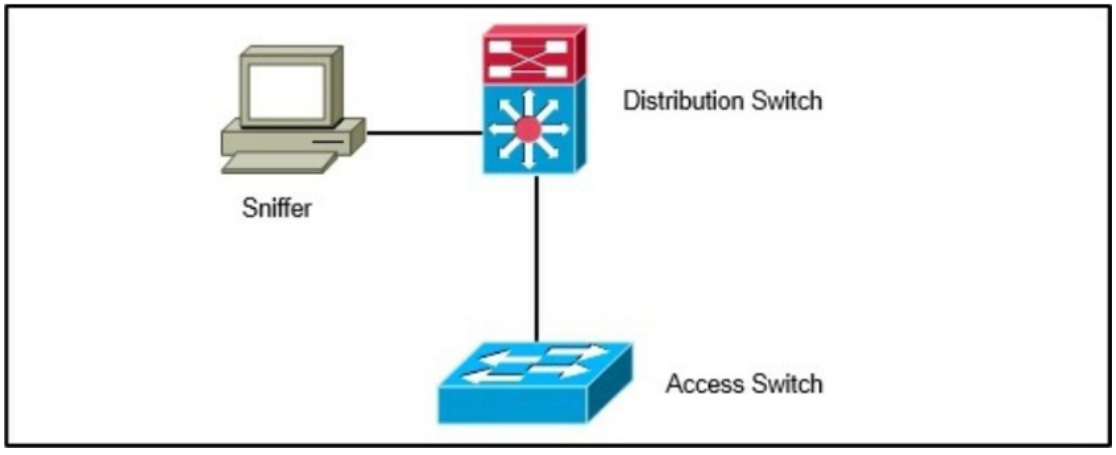
A. Change the configuration for GigabitEthernet0/48 so that it is a member of VLAN 10.
B. Add an access list to GigabitEthernet0/48 to filter out traffic that is not in VLAN 10.
C. Apply the monitor session filter globally to allow only traffic from VLAN 10.
D. Change the monitor session source to VLAN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

Correct Answer: C
Section: part1
Explanation

Explanation/Reference:
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#wp3 875419997

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: part1
Explanation

Explanation/Reference:

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: part1
Explanation

Explanation/Reference:
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 differ- ent switches in the switch stack (cross-stack EtherChannel).
desirable Places a port into an active negotiating state, in which the port starts negotia- tions with other ports by sending PAgP packets.
This mode is not supported when the EtherChannel members are from differ- ent 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 negotia- tions 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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:

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: part1
Explanation

Explanation/Reference:
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.

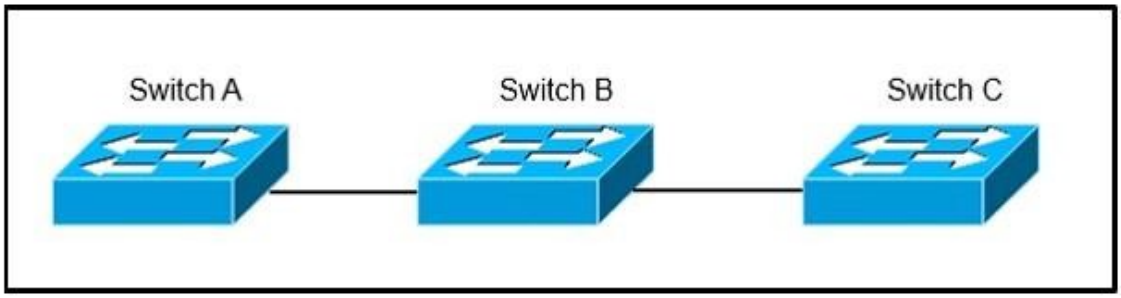
Correct Answer: B
Section: part1
Explanation

Explanation/Reference:
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?

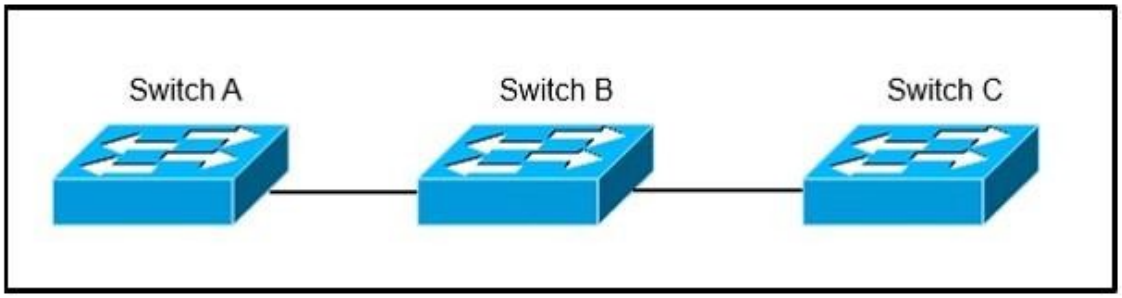
A. Switch B is configured in transparent mode.
B. Switch B is configured with an access port to Switch A, while Switch C is configured with a trunk port to Switch B.

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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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 Enters configuration mode. terminal Step 2 switch(config)# mac- Specifies the time before an entry ages out address-table aging- and is discarded from the MAC address table. time seconds [vlan The range is from 0 to 1000000; the default is vlan_id] 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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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: part1
Explanation

Explanation/Reference:
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