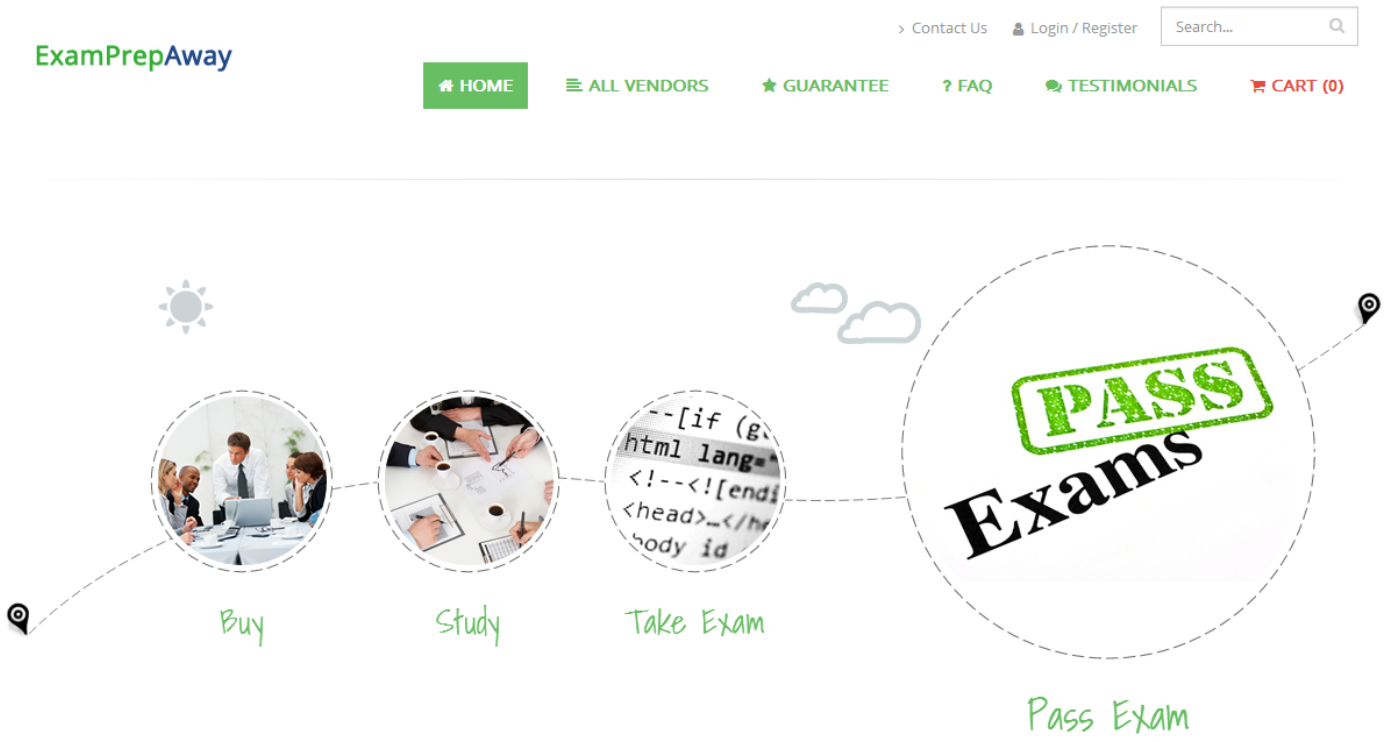
ExamPrepAway



Try **Online Engine** before you buy

We're not the only ones **happy** about ExamPrepAway Practice Material ...

56295+ customers in 100+ countries use ExamPrepAway Test Engine. Meet our customers.

GetCustom JET ORANGE iCompany Paradoxx iMessenger VOREED

http://www.examprepaway.com/

Latest Exam Guide & Learning Materials

Exam : **350-001**

Title : CCIE Routing and Switching Written

Vendor : Cisco

Version : DEMO

NO.1 Which statement is true about loop guard?
A. Loop guard only operates on interfaces that are considered point-to-point by the spanning tree.
B. Loop guard only operates on root ports.
C. Loop guard only operates on designated ports.
D. Loop guard only operates on edge ports.
Answer: A
Explanation:
Understanding How Loop Guard Works
Unidirectional link failures may cause a root port or alternate port to become designated as root if BPDUs are absent. Some software failures may introduce temporary loops in the network. Loop guard checks if a root port or an alternate root port receives BPDUs. If the port is receiving BPDUs, loop guard puts the port into an inconsistent state until it starts receiving BPDUs again. Loop guard isolates the failure and lets spanning tree converge to a stable topology without the failed link or bridge.
You can enable loop guard per port with the set spantree guard loop command.
Note When you are in MST mode, you can set all the ports on a switch with the set spantree global-defaults loop-guard command.
When you enable loop guard, it is automatically applied to all of the active instances or VLANs to which that port belongs. When you disable loop guard, it is disabled for the specified ports. Disabling loop guard moves all loop-inconsistent ports to the listening state.
If you enable loop guard on a channel and the first link becomes unidirectional, loop guard blocks the entire channel until the affected port is removed from the channel. Figure 8-6 shows loop guard in a triangle switch configuration.
Figure 8-6 Triangle Switch Configuration with Loop Guard

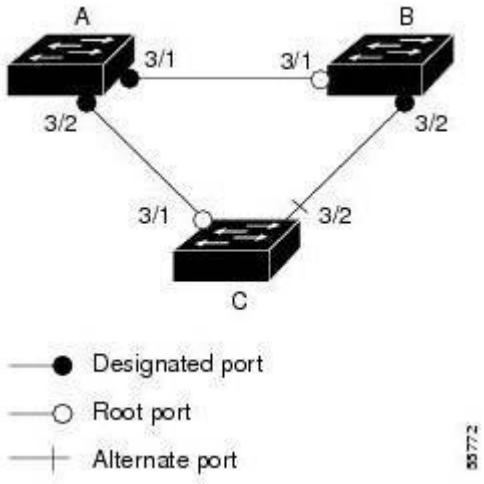
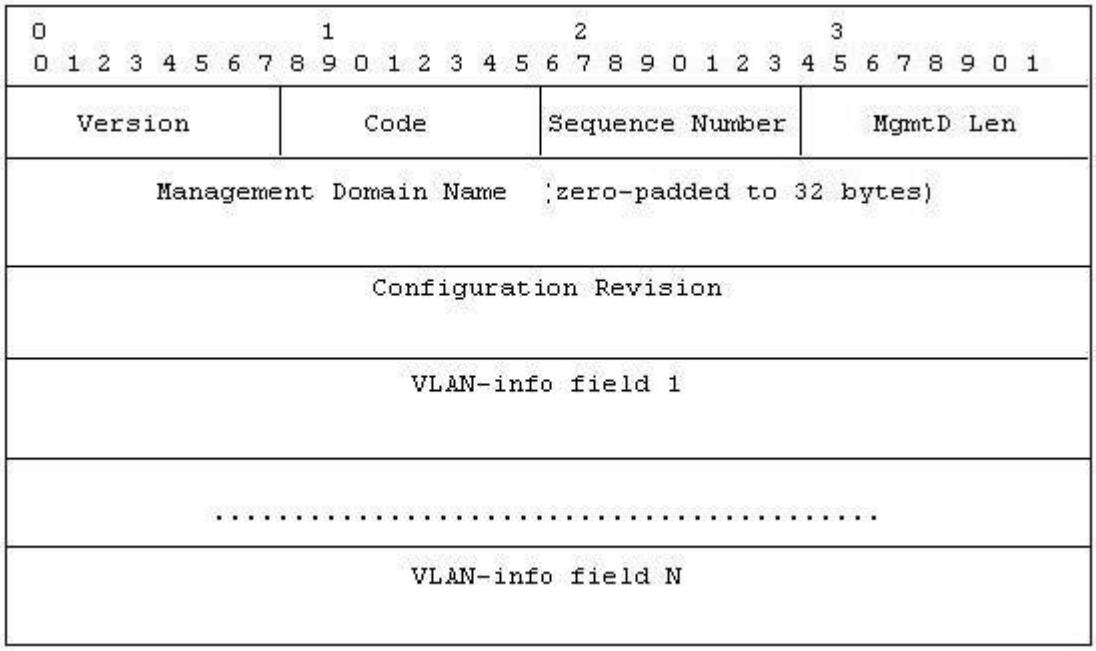


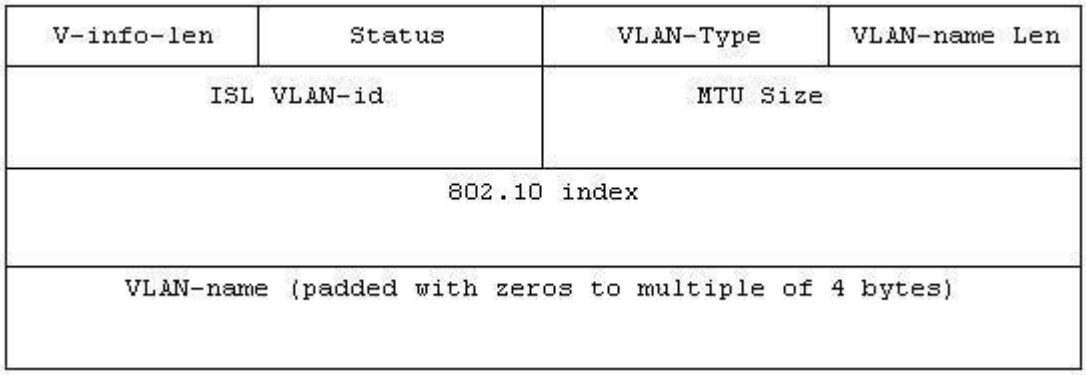
Figure 8-6 illustrates the following configuration:
Switches A and B are distribution switches.
Switch C is an access switch.
Loop guard is enabled on ports 3/1 and 3/2 on Switches A, B, and C.
Use loop guard only in topologies where there are blocked ports. Topologies that have no blocked ports, which are loop free, do not need to enable this feature. Enabling loop guard on a root switch has no effect but provides protection when a root switch becomes a nonroot switch.

Follow these guidelines when using loop guard:
Do not enable loop guard on PortFast-enabled or dynamic VLAN ports.
Do not enable PortFast on loop guard-enabled ports.
Do not enable loop guard if root guard is enabled.
Do not enable loop guard on ports that are connected to a shared link.
Note: We recommend that you enable loop guard on root ports and alternate root ports on access switches.
Loop guard interacts with other features as follows:
Loop guard does not affect the functionality of UplinkFast or BackboneFast.
Root guard forces a port to always be designated as the root port. Loop guard is effective only if the port is a root port or an alternate port. Do not enable loop guard and root guard on a port at the
same time.
PortFast transitions a port into a forwarding state immediately when a link is established. Because a PortFast-enabled port will not be a root port or alternate port, loop guard and PortFast cannot be configured on the same port. Assigning dynamic VLAN membership for the port requires that the port is PortFast enabled. Do not configure a loop guard-enabled port with dynamic VLAN membership. If your network has a type-inconsistent port or a PVID-inconsistent port, all BPDUs are dropped until the misconfiguration is corrected. The port transitions out of the inconsistent state after the message age expires. Loop guard ignores the message age expiration on type-inconsistent ports and PVID-inconsistent ports. If the port is already blocked by loop guard, misconfigured BPDUs that are received on the port make loop guard recover, but the port is moved into the type-inconsistent state or PVID-inconsistent state.
In high-availability switch configurations, if a port is put into the blocked state by loop guard, it remains blocked even after a switchover to the redundant supervisor engine. The newly activated supervisor engine recovers the port only after receiving a BPDU on that port. Loop guard uses the ports known to spanning tree. Loop guard can take advantage of logical ports provided by the Port Aggregation Protocol (PAgP). However, to form a channel, all the physical ports grouped in the channel must have compatible configurations. PAgP enforces uniform configurations of root guard or loop guard on all the physical ports to form a channel. These caveats apply to loop guard: -Spanning tree always chooses the first operational port in the channel to send the BPDUs. If that link becomes unidirectional, loop guard blocks the channel, even if other links in the channel are functioning properly. -If a set of ports that are already blocked by loop guard are grouped together to form a channel, spanning tree loses all the state information for those ports and the new channel port may obtain the forwarding state with a designated role. -If a channel is blocked by loop guard and the channel breaks, spanning tree loses all the state information. The individual physical ports may obtain the forwarding state with the designated role, even if one or more of the links that formed the channel are unidirectional. You can enable UniDirectional Link Detection (UDLD) to help isolate the link failure. A loop may occur until UDLD detects the failure, but loop guard will not be able to detect it. Loop guard has no effect on a disabled spanning tree instance or a VLAN.
Reference:
http://www.cisco.com/en/US/docs/switches/lan/catalyst4000/8.2glx/configuration/guide/stp_enha.html#wp1048163

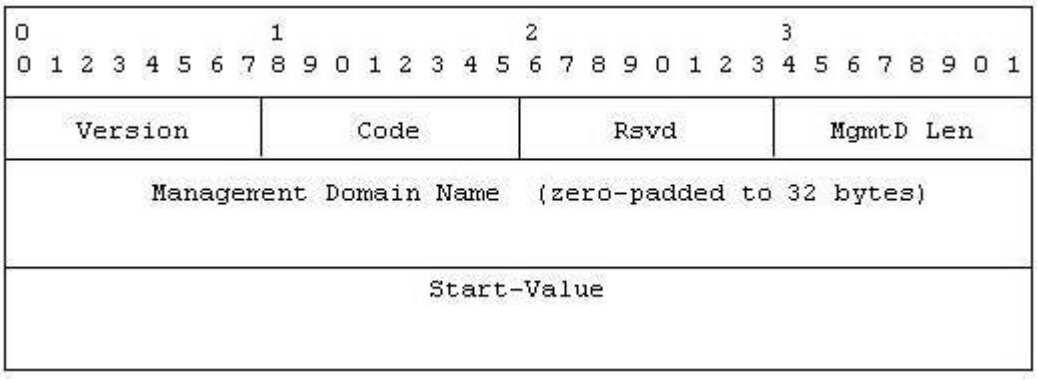
NO.2 Which command is used to enable EtherChannel hashing for Layer 3 IP and Layer 4 port-based CEF?
A. mpls ip cef
B. port-channel ip cef
C. mpls ip port-channel cef
D. port-channel load balance
E. mpls ip load-balance
F. ip cef EtherChannel channel-id XOR L4
G. ip cef connection exchange
Answer: D
Explanation:
Port-channel load balance is normally used for enable etherchannel hashing for Layer 3 IP and Layer 4 port based CEF.

NO.3 Which two options are contained in a VTP subset advertisement? (Choose two.)
A. followers field
B. MD5 digest
C. VLAN information
D. sequence number
Answer: C,D
Explanation:
Subset Advertisements When you add, delete, or change a VLAN in a Catalyst, the server Catalyst where the changes are made increments the configuration revision and issues a summary advertisement. One or several subset advertisements follow the summary advertisement. A subset advertisement contains a list of VLAN information.
If there are several VLANs, more than one subset advertisement can be required in order to advertise all the VLANs.
Subset Advertisement Packet Format This formatted example shows that each VLAN information field contains information for a different VLAN. It is ordered so that lowered-valued ISL VLAN IDs occur first:





Most of the fields in this packet are easy to understand. These are two clarifications:
Code - The format for this is 0x02 for subset advertisement.
Sequence number - This is the sequence of the packet in the stream of packets that follow a summary advertisement. The sequence starts with 1.
Advertisement Requests
A switch needs a VTP advertisement request in these situations:
The switch has been reset.
The VTP domain name has been changed.
The switch has received a VTP summary advertisement with a higher configuration revision than its own.
Upon receipt of an advertisement request, a VTP device sends a summary advertisement. One or more subset advertisements follow the summary advertisement. This is an example:



Code-The format for this is 0x03 for an advertisement request.
Start-Value-This is used in cases in which there are several subset advertisements. If the first (n) subset advertisement has been received and the subsequent one (n+1) has not been received, the Catalyst only requests advertisements from the (n+1)th one.
Reference
http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml

NO.4 Which two statements are true about traffic shaping? (Choose two.)
A. Out-of-profile packets are queued.
B. It causes TCP retransmits.
C. Marking/remarking is not supported.
D. It does not respond to BECN and ForeSight Messages.
E. It uses a single/two-bucket mechanism for metering.
Answer: A,C
Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCwQFjAA&url=http%3A%2F%2Fstaffweb.itsligo.ie%2Fstaff%2Fpflynn%2FTelecoms%25203%2FSlides%2FONT%2520Mod%25204%2520Lesson%25207.ppt&ei=LoDIUfTTGtO3hAeQz4HQCA&usg=AFQjCNGY24UkAfy8tKIHlzEm9gfoIjv6fg&sig2=t4UIzkZ12wnO2988dEDyug&bvm=bv.48293060,d.ZG4 (slide 6)

NO.5 Which three options are features of VTP version 3? (Choose three.)
A. VTPv3 supports 8K VLANs.
B. VTPv3 supports private VLAN mapping.
C. VTPv3 allows for domain discovery.
D. VTPv3 uses a primary server concept to avoid configuration revision issues.
E. VTPv3 is not compatible with VTPv1 or VTPv2.
F. VTPv3 has a hidden password option.
Answer: B,D,F
Explanation:
Key Benefits of VTP Version 3 Much work has gone into improving the usability of VTP version 3 in three major areas: The new version of VTP offers better administrative control over which device is allowed to update other devices' view of the VLAN topology. The chance of unintended and disruptive changes is significantly reduced, and availability is increased. The reduced risk of unintended changes will ease the change process and help speed deployment. Functionality for the

VLAN environment has been significantly expanded. Two enhancements are most beneficial for today's networks:

-
In addition to supporting the earlier ISL VLAN range from 1 to 1001, the new version supports the whole IEEE 802.1Q VLAN range up to 4095.

-
In addition to supporting the concept of normal VLANs, VTP version 3 can transfer information regarding Private VLAN (PVLAN) structures.

The third area of major improvement is support for databases other than VLAN (for example, MST).

Brief Background on VTP Version 1 and VTP Version 2 VTP version 1 was developed when only 1k VLANs where available for configuration. A tight internal coupling of the VLAN implementation, the VLAN pruning feature, and the VTP function itself offered an efficient means of implementation. It has proved in the field to reliably support Ethernet, Token Ring, and FDDI networks via VTP. The use of consistent VLAN naming was a requirement for successful use of VMPS (Vlan Membership Policy Server). VTP ensures the consistency of VLAN names across the VTP domain. Most VMPS implementations are likely to be migrated to a newer, more flexible and feature-rich method. To add support for Token Ring, VTP version 1 was enhanced and called VTP version 2. Certain other minor changes and enhancements were also added at this time. The functional base in VTP version 3 is left unchanged from VTP version 2, so backward compatibility is built in. It is possible, on a per link basis, to automatically discover and support VTP version 2 devices.

VTP version 3 adds a number of enhancements to VTP version 1 and VTP version 2: Support for a structured and secure VLAN environment (Private VLAN, or PVLAN) Support for up to 4k VLANs Feature enhancement beyond support for a single database or VTP instance Protection from unintended database overrides during insertion of new switches Option of clear text or hidden password protection Configuration option on a per port base instead of only a global scheme Optimized resource handling and more efficient transfer of information These new requirements made a new code foundation necessary. The design goal was to make VTP version 3 a versatile vehicle. This was not only for the task of transferring a VLAN DB but also for transferring other databases-for example, the MST database.

Reference

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/solution_guide_c78_508010.ht ml

NO.6 Which three options are considered in the spanning-tree decision process? (Choose three.)

A. lowest root bridge ID

B. lowest path cost to root bridge

C. lowest sender bridge ID

D. highest port ID

E. highest root bridge ID

F. highest path cost to root bridge

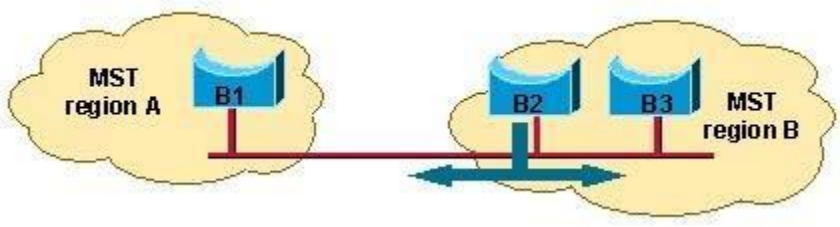
Answer: A,B,C

Explanation:

Configuration bridge protocol data units (BPDUs) are sent between switches for each port. Switches

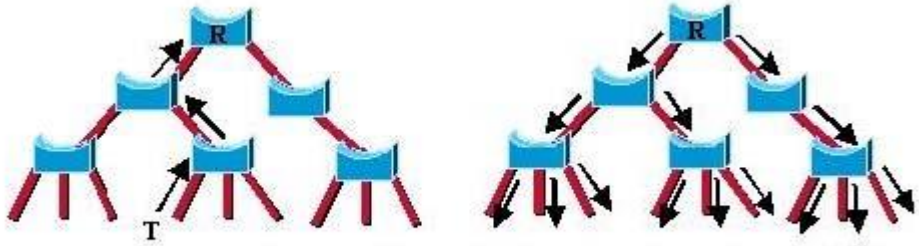
use s four step process to save a copy of the best BPDU seen on every port. When a port receives a better BPDU, it stops sending them. If the BPDUs stop arriving for 20 seconds (default), it begins sending them again.
Step 1 Lowest Root Bridge ID (BID) Step 2 Lowest Path Cost to Root Bridge Step 3 Lowest Sender BID Step 4 Lowest Port ID
Reference Cisco General Networking Theory Quick Reference Sheets

NO.7 In 802.1s, how is the VLAN to instance mapping represented in the BPDU?
A. The VLAN to instance mapping is a normal 16-byte field in the MST BPDU.
B. The VLAN to instance mapping is a normal 12-byte field in the MST BPDU.
C. The VLAN to instance mapping is a 16-byte MD5 signature field in the MST BPDU.
D. The VLAN to instance mapping is a 12-byte MD5 signature field in the MST BPDU.
Answer: C
Explanation:
MST Configuration and MST Region Each switch running MST in the network has a single MST configuration that consists of these three attributes:
1.An alphanumeric configuration name (32 bytes)
2.A configuration revision number (two bytes)
3.A 4096-element table that associates each of the potential 4096 VLANs supported on the chassis to a given instance.
In order to be part of a common MST region, a group of switches must share the same configuration attributes. It is up to the network administrator to properly propagate the configuration throughout the region. Currently, this step is only possible by the means of the command line interface (CLI) or through Simple Network Management Protocol (SNMP). Other methods can be envisioned, as the IEEE specification does not explicitly mention how to accomplish that step. Note: If for any reason two switches differ on one or more configuration attribute, the switches are part of different regions. For more information refer to the Region Boundary section of this document.
Region Boundary In order to ensure consistent VLAN-to-instance mapping, it is necessary for the protocol to be able to exactly identify the boundaries of the regions. For that purpose, the characteristics of the region are included in the BPDUs. The exact VLANs-to-instance mapping is not propagated in the BPDU, because the switches only need to know whether they are in the same region as a neighbor. Therefore, only a digest of the VLANs-toinstance mapping table is sent, along with the revision number and the name. Once a switch receives a BPDU, the switch extracts the digest (a numerical value derived from the VLAN-to-instance mapping table through a mathematical function) and compares this digest with its own computed digest. If the digests differ, the port on which the BPDU was received is at the boundary of a region. In generic terms, a port is at the boundary of a region if the designated bridge on its segment is in a different region or if it receives legacy 802.1d BPDUs. In this diagram, the port on B1 is at the boundary of region A, whereas the ports on B2 and B3 are internal to region B:



MST Instances
According to the IEEE 802.1s specification, an MST bridge must be able to handle at least these two instances:
One Internal Spanning Tree (IST)
One or more Multiple Spanning Tree Instance(s) (MSTIs)
The terminology continues to evolve, as 802.1s is actually in a pre-standard phase. It is likely these names will change in the final release of 802.1s. The Cisco implementation supports 16 instances: one IST (instance 0) and 15 MSTIs.
show vtp status
Cisco switches "show vtp status" Field Descriptions has a MD5 digest field that is a 16-byte checksum of the
VTP configuration as shown below
Router# show vtp status
VTP Version: 3 (capable)
Configuration Revision: 1
Maximum VLANs supported locally: 1005
Number of existing VLANs: 37
VTP Operating Mode: Server
VTP Domain Name: [smartports]
VTP Pruning Mode: Disabled
VTP V2 Mode: Enabled VTP Traps Generation: Disabled MD5 digest : 0x26 0xEE 0x0D 0x84 0x73 0x0E 0x1B 0x69 Configuration last modified by 172.20.52.19 at 7-25-08 14:33:43 Local updater ID is 172.20.52.19 on interface Gi5/2 (first layer3 interface fou) VTP version running: 2
Reference
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfc.shtml http://www.cisco.com/en/US/docs/ios-xml/ios/lanswitch/command/lsw-cr-book.pdf

NO.8 Which statement is true about TCN propagation?
A. The originator of the TCN immediately floods this information through the network.
B. The TCN propagation is a two step process.
C. A TCN is generated and sent to the root bridge.
D. The root bridge must flood this information throughout the network.
Answer: C
Explanation:
Explanation New Topology Change Mechanisms When an 802.1D bridge detects a topology change, it uses a reliable mechanism to first notify the root bridge. This is shown in this diagram:



A topology change is generated on point T.
1st step: A TCN is going up to the root.

2nd step: the root advertises the TC for max-age+ forward delay.

Once the root bridge is aware of a change in the topology of the network, it sets the TC flag on the BPDUs it sends out, which are then relayed to all the bridges in the network. When a bridge receives a BPDU with the TC flag bit set, it reduces its bridging-table aging time to forward delay seconds. This ensures a relatively quick flush of stale information. Refer to Understanding Spanning-Tree Protocol Topology Changes for more information on this process. This topology change mechanism is deeply remodeled in RSTP. Both the detection of a topology change and its propagation through the network evolve.

Topology Change Detection

In RSTP, only non-edge ports that move to the forwarding state cause a topology change. This means that a loss of connectivity is not considered as a topology change any more, contrary to 802.1D (that is, a port that moves to blocking no longer generates a TC). When a RSTP bridge detects a topology change, these occur:

It starts the TC While timer with a value equal to twice the hello-time for all its non-edge designated ports and its root port, if necessary.

It flushes the MAC addresses associated with all these ports.

Note: As long as the TC While timer runs on a port, the BPDUs sent out of that port have the TC bit set.

BPDUs are also sent on the root port while the timer is active.

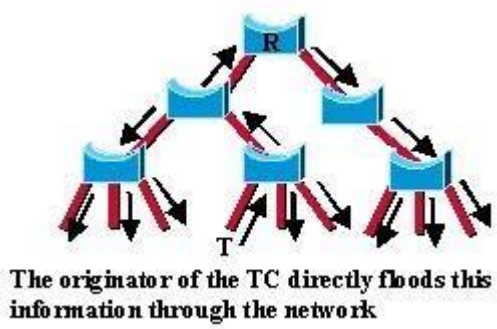
Topology Change Propagation

When a bridge receives a BPDU with the TC bit set from a neighbor, these occur:

It clears the MAC addresses learned on all its ports, except the one that receives the topology change.

It starts the TC While timer and sends BPDUs with TC set on all its designated ports and root port (RSTP no longer uses the specific TCN BPDU, unless a legacy bridge needs to be notified).

This way, the TCN floods very quickly across the whole network. The TC propagation is now a one step process. In fact, the initiator of the topology change floods this information throughout the network, as opposed to 802.1D where only the root did. This mechanism is much faster than the 802.1D equivalent. There is no need to wait for the root bridge to be notified and then maintain the topology change state for the whole network for <max age plus forward delay> seconds.



In just a few seconds, or a small multiple of hello-times, most of the entries in the CAM tables of the entire network (VLAN) flush. This approach results in potentially more temporary flooding, but on the other hand it clears potential stale information that prevents rapid connectivity restitution.
Reference
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml

NO.9 While you are troubleshooting network performance issues, you notice that a switch is periodically flooding all unicast traffic. Further investigation reveals that periodically the switch is also having spikes in CPU utilization, causing the MAC address table to be flushed and relearned. What is the most likely cause of this issue?
A. a routing protocol that is flooding updates
B. a flapping port that is generating BPDUs with the TCN bit set
C. STP is not running on the switch
D. a user that is downloading the output of the show-tech command
E. a corrupted switch CAM table
Answer: B
Explanation:
Spanning-Tree Protocol Topology Changes Another common issue caused by flooding is Spanning-Tree Protocol (STP) Topology Change Notification (TCN). TCN is designed to correct forwarding tables after the forwarding topology has changed. This is necessary to avoid a connectivity outage, as after a topology change some destinations previously accessible via particular ports might become accessible via different ports. TCN operates by shortening the forwarding table aging time, such that if the address is not relearned, it will age out and flooding will occur. TCNs are triggered by a port that is transitioning to or from the forwarding state. After the TCN, even if the particular destination MAC address has aged out, flooding should not happen for long in most cases since the address will be relearned. The issue might arise when TCNs are occurring repeatedly with short intervals. The switches will constantly be fast-aging their forwarding tables so flooding will be nearly constant. Normally, a TCN is rare in a well-configured network. When the port on a switch goes up or down, there is eventually a TCN once the STP state of the port is changing to or from forwarding. When the port is flapping, repetitive TCNs and flooding occurs. Ports with the STP portfast feature enabled will not cause TCNs when going to or from the forwarding state. Configuration of portfast on all end-device ports (such as printers, PCs, servers, and so on) should limit TCNs to a low amount. Refer to this document for more information on TCNs: Understanding Spanning-Tree Protocol Topology Changes Note: In MSFC IOS, there is an

optimization that will trigger VLAN interfaces to repopulate their ARP tables when there is a TCN in the respective VLAN. This limits flooding in case of TCNs, as there will be an ARP broadcast and the host MAC address will be relearned as the hosts reply to ARP.
Reference
http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a00801d0808. shtml

NO.10 Your network is suffering from regular outages. After troubleshooting, you learn that the transmit lead of a fiber uplink was damaged. Which two features can prevent the same issues in the future? (Choose two.)
A. root guard
B. loop guard
C. BPDU guard
D. UDLD
E. BPDU skew detection
Answer: B,D
Explanation:
STP Loop Guard The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs. When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes designated and moves to a forwarding state. This situation creates a loop. The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the designated port role. The port moves to the STP forwarding state and creates a loop.
Loop Guard versus UDLD Loop guard and Unidirectional Link Detection (UDLD) functionality overlap, partly in the sense that both protect against STP failures caused by unidirectional links. However, these two features differ in functionality and how they approach the problem. This table describes loop guard and UDLD functionality:

Functionality	Loop Guard	UDLD
Configuration	Per-port	Per-port
Action granularity	Per-VLAN	Per-port
Autorecover	Yes	Yes, with err-disable timeout feature
Protection against STP failures caused by unidirectional links	Yes, when enabled on all root and alternate ports in redundant topology	Yes, when enabled on all links in redundant topology
Protection against STP failures caused by problems in the software (designated switch does not send BPDU)	Yes	No
Protection against miswiring.	No	Yes

Based on the various design considerations, you can choose either UDLD or the loop guard feature. In regards to STP, the most noticeable difference between the two features is the absence of protection in UDLD against STP failures caused by problems in software. As a result, the designated switch does not send BPDUs. However, this type of failure is (by an order of magnitude) more rare than failures caused by unidirectional links. In return, UDLD might be more flexible in the case of unidirectional links on EtherChannel. In this case, UDLD disables only failed links, and the channel should remain functional with the links that remain. In such a failure, the loop guard puts it into loop-inconsistent state in order to block the whole channel.
Additionally, loop guard does not work on shared links or in situations where the link has been unidirectional since the link-up. In the last case, the port never receives BPDU and becomes designated. Because this behavior could be normal, this particular case is not covered by loop guard. UDLD provides protection against such a scenario. As described, the highest level of protection is provided when you enable UDLD and loop guard.
Reference
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a0080094640.shtml#loop_guard_vs_uld