350-001

CCIE Cisco Certified Internetworking Expert

DEMO

Topic 1, Implement Layer 2 Technologies

QUESTION 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 span tree guard loop command.

Note When you are in MST mode, you can set all the ports on a switch with the set span tree 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

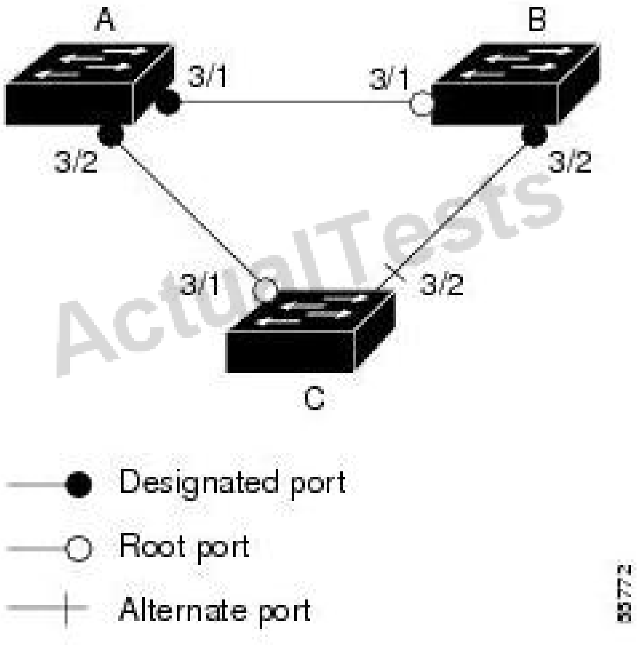

Figure 8-6 illustrates the following configuration:
Switches A and B are distribution switches.
Switch C is an access switch.
Loop guard is enabled on ports 3/1 and 3/2 on Switches A, B, and C.
Use loop guard only in topologies where there are blocked ports. Topologies that have no blocked ports, which 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.

QUESTION 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