

Chapter 10:

Protecting the Spanning Tree Topology

- Protecting Against Unexpected BPDUs
- Protecting Against Sudden Loss of BPDUs
 - Troubleshooting STP Protection

Protecting Against Unexpected BPDUs

- Protecting the stable STP Topology when a foreign or rogue switch is introduced.
- Two Features are available for Catalyst Switches
 - Root Guard
 - BPDU guard

Root Guard - Overview

- The traditional STP does not provide any means for the network administrator to securely enforce the topology of the switched Layer 2 (L2) network.
- This may become especially important in networks with shared administrative control, for example, one switched network controlled by different administrative entities or companies.

Root Guard - Overview

- Forwarding topology of the switched network is calculated on the root bridge position.
- Although any switch can be root bridge in the network, it is better to place the root bridge manually (core layer) so the forwarding topology will be more optimal.
- **Standard STP does not allow the administrator to enforce the position of the root bridge.**
 - If there will be a bridge in the network with lower bridge priority it will take the role of the root bridge.

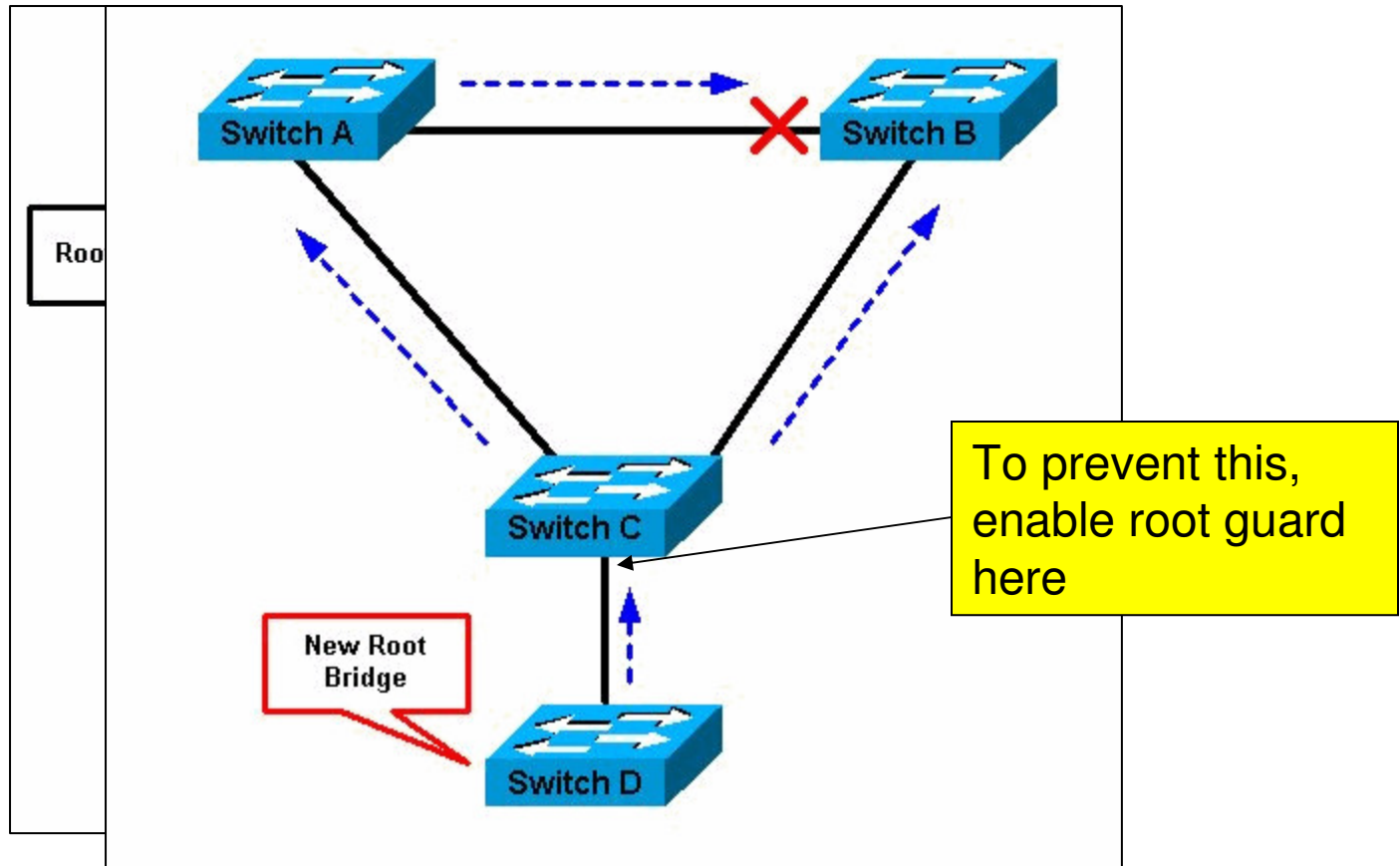
Root Guard

- Even if the administrator sets the root bridge priority to zero in an effort to secure the root bridge position, there is still no guarantee, as there might be a bridge with **priority zero** and a **lower bridge ID**.
- Root guard feature is designed to provide a way to enforce the root bridge placement in the network.

Root Guard - Operation

- The root guard ensures that the port on which it is enabled is the designated port.
- If the bridge receives superior STP BPDUs on a root guard enabled port, this port will be moved to a root-inconsistent STP state (effectively equal to listening state), and no traffic will be forwarded across this port.
- The position of the root bridge will be enforced.

Root Guard - Example



Root Guard - Configuration

- Root Guard is enabled on a per port basis

```
Switch(config-if)# spanning-tree guard root
```

- Use root guard on ports that you **NEVER** expect to find the Root Bridge for a VLAN
- Root guard designates that a port can only relay BPDUs and not receive them

BPDU Guard

- Used on Access Layer switches.
- Configured on ports with portfast enabled (the port is attached to an end node device that WILL NOT send BPDUs).
- Protects the stable STP topology from being disrupted by a foreign or rogue switch.
 - Works by putting the port into the *errdisable* state when ANY BPDUs are received.

```
Switch(config-if)# spanning-tree bpduguard enable
```

Chapter 11: Protecting the Spanning Tree Topology

- Protecting Against Unexpected BPDUs
- Protecting Against Sudden Loss of BPDUs
 - Troubleshooting STP Protection

BPDUs Loss

- In a stable STP topology, BPDUs are still being sent (responsive).
- What happens when switch ports that have been receiving BPDUs start receiving them late or not at all?
- Blocked ports can become unblocked causing loops to form.

Solutions to the Loss of BPDUs

- Cisco has three features that detect or prevent STP topology changes due to the loss or delay of BPDUs.
 - Loop Guard
 - Unidirectional Link Detection (UDLD)

Loop Guard

- Is used to detect the loss of BPDUs on a blocked port AND prevent that port from moving into the forwarding state (causing a bridging loop).
 - A switch port is receiving BPDUs
 - It is not the Root Port or Designated Port – therefore, it is in the blocking state.
 - The port stops receiving BPDUs
 - The BPDUs are kept for ? Seconds (default)
 - When the Max-age timer expires, the switch will think that it can move through the STP state sequence to the forwarding state.
 - A bridging loop will form.

Loop Guard

- When BPDUs go missing, Loop Guard moves the port into a new state called *loop-inconsistent* state.
 - This state keeps the port in a blocking but monitors the port for the resumption of BPDUs
 - If/When BPDUs resume, the port is allowed to move through the STA in order to get to an acceptable state/role for the topology.
- Loop Guard is enabled on a per port basis

```
Switch(config-if)# spanning-tree guard loop
```

Unidirectional Link Detection (UDLD)

- Typically, switches are connected together with bi-directional links.
- If a physical layer problem develops that causes one of the communication channels to be disrupted and therefore disrupting the flow of traffic in one direction.
- A potential danger to the STP topology exists because BPDUs may not be received on one end of the link.

Unidirectional Link Detection (UDLD)

- To prevent this situation from corrupting the STP topology, UDLD can be enabled.
- UDLD monitors the link to make sure traffic is flowing in both directions.
 - UDLD sends special frames that identify the switch port.
 - UDLD expects those frames to be echoed back with the far end's switch port added.
 - If a frame is received on the sending switch with both its and the neighbors ports identified – a bidirectional path exists

Unidirectional Link Detection (UDLD)

- This means that BOTH ends of the link must be configured for UDLD in order for to participate in the echo process.
- In order to detect a unidirectional link before it has affected the STP state, the time frame for the three-way exchange must be less than the STP time to move from a Blocked to a Forward state (50 seconds – 15 + 15 + 20)
- Therefore, the default interval for UDLD frames is 15 seconds (15 + 15 + 15 = 45)

Unidirectional Link Detection (UDLD)

- UDLD has two modes that it can operate in.
 - Normal mode:
 - After a unidirectional link condition is detected, the port is allowed to continue its operation.
 - It marks the condition and generates a syslog message
 - Aggressive mode:
 - After a unidirectional link condition is detected, the switch takes action to re-establish the link.
 - UDLD frames are sent out once per second for eight seconds.
 - If none are echoed, the port is put into errdisable state.

Configuring UDLD

- UDLD is usually configured for fiber-optic ports because copper media does not suffer from the physical conditions that allow a unidirectional link to form (LED going bad).
- UDLD is configured on a per-port basis
 - Can be globally enabled for all fiber switch ports
 - By default, UDLD is disabled on all ports

Configuring UDLD

```
Switch(config)# udld {aggressive | enable | message time seconds}
```

- For Normal mode – use the enable keyword
- For Aggressive mode – use the aggressive keyword
- To set the time interval – use the message time key word
 - can adjust the interval from 7 to 90 seconds
 - Catalyst 2950/3550 – default is 7 seconds
 - Catalyst 4500/6500 – default is 15 seconds

Troubleshooting STP Protection

Display Function	Command Syntax
List the ports that have been labeled in an inconsistent state	show spanning-tree inconsistentports
Look for detailed reasons for inconsistencies	show spanning-tree interface <i>type mod/num</i> [detail]
Display the Global BPDU guard state	show spanning-tree summary
Display the UDLD status on one or all ports	show udd [<i>type mod/num</i>]
Re-enable ports that UDLD aggressive mode has errdisabled	udd reset