Configuring Loop Detection Guard

- Restrictions for Loop Detection Guard, on page 1
- Information About Loop Detection Guard, on page 1
- Enabling Loop Detection Guard and Error-Disabling the Required Port, on page 4
- Additional References for Configuring Loop Detection Guard, on page 5
- Feature History for Loop Detection Guard, on page 5

Restrictions for Loop Detection Guard

Loop detection guard can be configured only on Layer 2 physical interfaces. Layer 3 ports and virtual interfaces, such as port channels, switch virtual interfaces (SVIs), and tunnels, are not supported.

Information About Loop Detection Guard

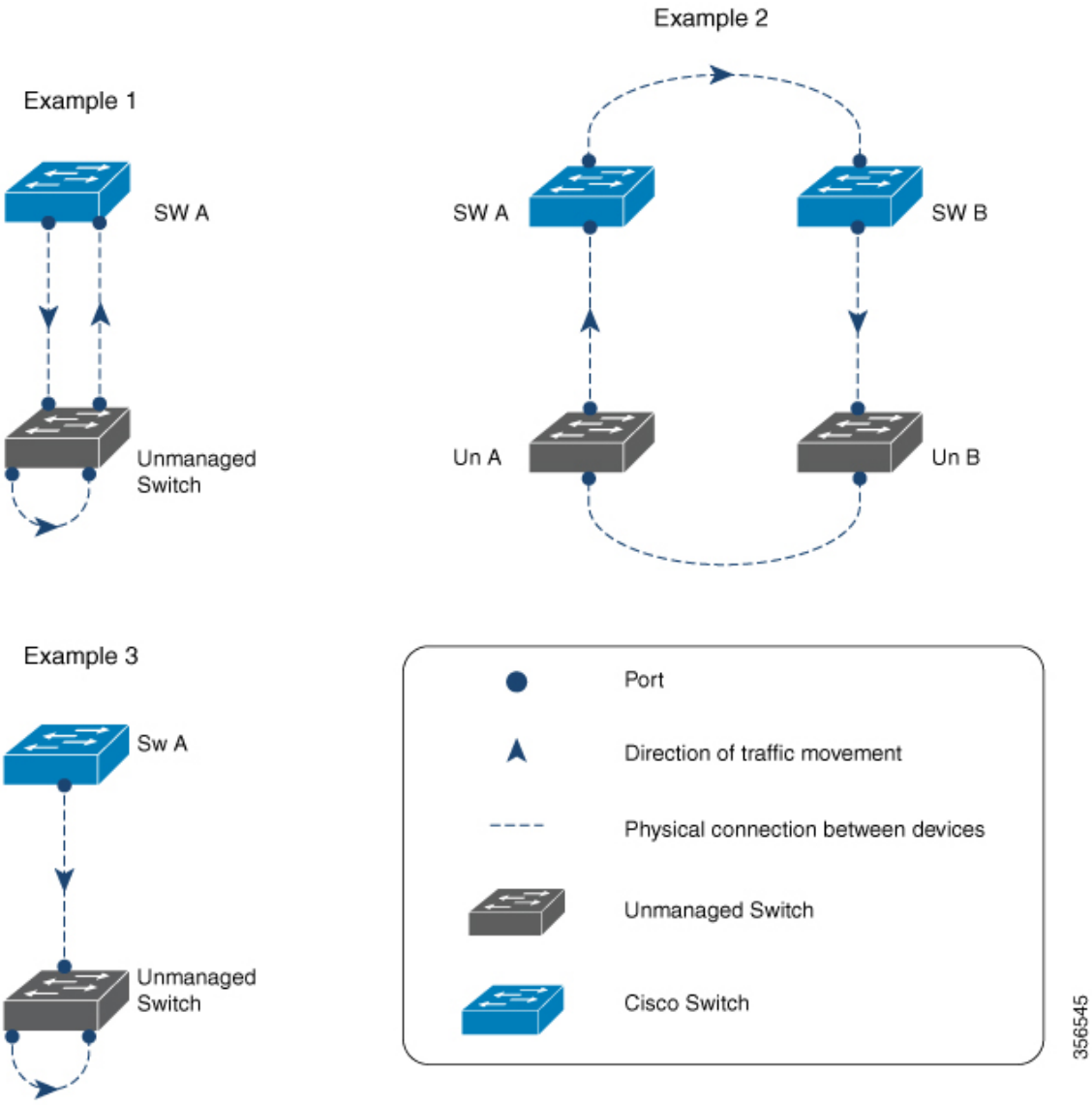
A computer network can experience a network loop where there is more than one Layer 2 path between two endpoints. This is possible when there are multiple connections between two switches in a network or two ports on the same switch are connected to each other. The following figure shows a few examples of a network loop:

Example 1: Switch SW A, which is within the network, is sending traffic to an unmanaged switch on one port and receiving traffic from the same unmanaged switch, on another port. On the unmanaged switch, the port receiving traffic is connected to the port sending traffic back to the SW A in the network, resulting in a network loop.

Example 2: This example shows a network loop involving four switches, two within the network (SW A and SW B) and two unmanaged switches (Un A and Un B). Traffic is moving in the following direction SW A to SW B to Un B to Un A and back to SW A, resulting in a network loop.

Example 3: Two ports on the unmanaged switch are connected to each other, resulting in a network loop.

Figure 1: Examples of Network Loop Between Managed and Unmanaged Switches



While Spanning Tree Protocol (STP) is normally the protocol that is configured for this purpose (to prevent network loops), loop detection guard is suited to situations where there may be unmanaged switches in a network that do not understand STP, or where STP is not configured on the network.

Loop detection guard is enabled at the interface level. To detect loops, the system sends loop-detect frames from the interface, at preconfigured intervals. When a loop is detected, the configured action is taken.

Loop detection guard is disabled by default. When you enable the feature, you can configure one of these actions:

- Error-disable the port sending traffic.
- Error-disable the port receiving traffic (default).
- Display an error message and not disable any port.

When a port is error-disabled, no traffic is sent or received on that port.

Interaction of Loop Detection Guard with Other Features

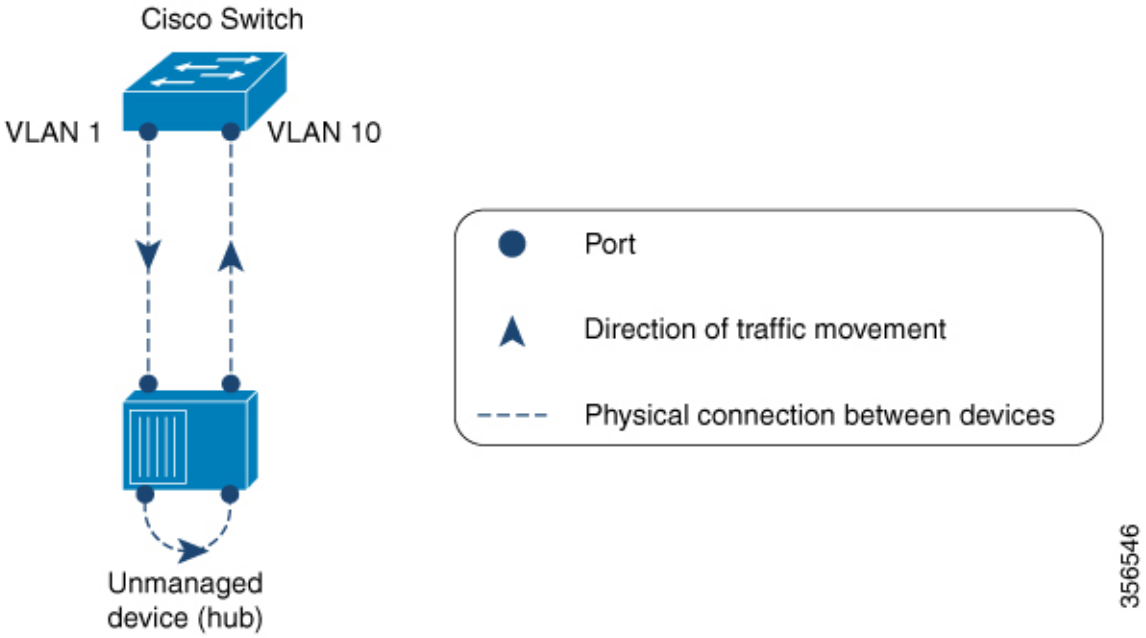
Spanning Tree Protocol and Loop Detection Guard

When both loop detection guard and STP are enabled on a device, STP takes over monitoring the network for loops. In this case loop-detect packets are neither received nor processed in the network.

VLANs and Loop Detection Guard

We do not recommend configuring this feature on a switch that is connected to a hub for these reasons: The hub floods traffic to all of its interfaces. If the switch in your network is receiving traffic from the same hub, but on a port in a different VLAN, you may be inadvertently error-disabling those destination ports. The figure below illustrates such a situation. The port in VLAN 1 is sending traffic to the hub. The switch is also receiving traffic from the same hub, but on a port in a different VLAN, that is, VLAN 10. If you configure loop detection guard (and you have configured the default action of error-disabling the destination port), then the port in VLAN 10 is blocked. Configuring the option to display a message (instead of error-disabling a port) is not recommended either, because the system displays as many messages as the number of interfaces configured in the hub, resulting in a CPU overload.

Figure 2: A Switch Connected to an Unmanged Network Hub



Enabling Loop Detection Guard and Error-Disabling the Required Port

The feature is disabled by default. Complete the following steps to enable loop detection guard and configure the action that you want the system to take when a loop is detected:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**interface** {*interface-id* | *subinterface-id* | *vlan-id*}
	Example:
	`Device(config)# interface tengigabitethernet 1/0/20`
	`Device(config-if)#`
		Enters interface configuration mode. Specify only a physical interface to configure loop detection guard on the device. Layer 3 ports and virtual interfaces like PortChannels, switch virtual interfaces (SVIs), and tunnels are not supported.

Step 4	[**no**] **loopdetect** **Example:** `Device(config-if)# loopdetect`	Enables loop detection guard on the device. Loopdetect frames are sent from the configured interface. Use the **loopdetect** command without any keyword to enable loop detection guard. Use the **no** form of this command to disable this feature. **Note** You can enable the feature on trunk ports, but a warning message is displayed, for the following reason: A trunk port carries traffic for several VLANs, simultaneously. A loop that is detected in one VLAN can result in the error-disabling of all VLAN traffic that is associated with the trunk port.
Step 5	[**no**] **loopdetect** {*time* | **action syslog** | **source-port**} **Example:** `Device(config-if)# loopdetect 7`	Specifies the frequency at which loop-detect frames are sent and the action the system takes when a loop is detected. If you do not specify an action, the destination port is error-disabled by default. You can configure the following:

	Command or Action	Purpose
		• *time*—Time interval to send loop-detect frame, in seconds. The range is from 1 to 10. The default is 5. • **action syslog**—Displays a system message and does not error-disable any port. If you use the **no** form of this command, the system reverts to the last configured option. • **source-port**—Error-disables the source port. If you use the **no** form of this command, the destination port is error-disabled. In the example configuration on the left (`Device(config-if)# loopdetect 7`), the interface is configured to send loop-detect frames every 7 seconds, and to error-disable the destination port if a loop is detected (The default applies, because neither the **action syslog** option nor the **source-port** option has been configured).
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show loopdetect** **Example:** `Device# show loopdetect`	Displays all the interfaces where loop detection guard is enabled, the frequency at which loop-detect packets are sent, and the status of the physical interface.

Additional References for Configuring Loop Detection Guard

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	See the Layer 2/3 Commands section of the *Command Reference (Catalyst 9200 Series Switches)*

Feature History for Loop Detection Guard

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.2.1	Loop Detection Guard	Loop detection guard prevents network loops in either networks that are not configured with STP or unmanaged devices in networks that are configured with STP.
Cisco IOS XE Cupertino 17.9.1	Loop Detection Guard	This feature was implemented on C9200CX-12P-2X2G, C9200CX-8P-2X2G, and C9200CX-12T-2X2G models of the Cisco Catalyst 9200CX Series Switches, which were introduced in this release.”

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.