CHAPTER 35

Configuring Control-Plane Security

In any network, Layer 2 and Layer 3 switches exchange control packets with other switches in the network. The Cisco CGS 2520 switch, which acts as a transition between the customer network and the service-provider network, uses control-plane security to ensure that the topology information between the two networks is isolated. This mechanism protects against a possible denial-of-service attack from another customer network.

Understanding Control-Plane Security

In the Cisco CGS 2520 switch, ports configured as network node interfaces (NNIs) connect to the service-provider network. The switch communicates with the rest of the network through these ports, exchanging protocol control packets as well as regular traffic. Other ports on the Cisco CGS 2520 switch are user network interfaces (UNIs) that are used as customer-facing ports. Each port is connected to a single customer, and exchanging network protocol control packets between the switch and the customer is not usually required. Most Layer 2 protocols are not supported on UNIs. To protect against accidental or intentional CPU overload, the Cisco CGS 2520 switch provides control-plane security automatically by dropping or rate-limiting a predefined set of Layer 2 control packets and some Layer 3 control packets for UNIs.

You can also configure a third port type, an enhanced network interface (ENI). An ENI, like a UNI, is a customer-facing interface. By default on an ENI, Layer 2 control protocols, such as Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP) are disabled. On ENIs, unlike UNIs, you can enable these protocols. When configuring ENIs in port channels, you can also enable Link Aggregation Control Protocol (LACP), and Port Aggregation Protocol (PAgP). ENIs drop or rate-limit the protocol packets, depending on whether the protocol is enabled or disabled on the interface. For all other control protocols on ENIs, the switch drops or rate-limits packets the same way as it does for UNIs.

CPU protection, which is enabled by default, uses 19 policers per port. When it is enabled, you can configure a maximum of 45 policers per port. If you need to configure more policers per port, you can disable CPU protection by entering the **no policer cpu uni all** global configuration command and reloading the switch. When CPU protection is disabled, you can configure a maximum of 63 policers per port for user-defined classes and one for class-default.

Note When CPU is turned off, protocol packets can reach the CPU, which could cause CPU processing overload and storm control through software.

Control-plane security is supported on a port for Layer 2 control packets and non-IP packets with router MAC addresses, regardless of whether the port is in routing or nonrouting mode. (A port is in routing mode when global IP routing is enabled and the port is configured with the **no switchport** interface configuration command or is associated with a VLAN that has an active switch virtual interface [SVI].) These packets are either dropped or rate-limited, depending upon the Layer 2 protocol configuration. For Layer 3 control packets, on a port in routing mode (whether or not a Layer 3 service policy is attached), control-plane security supports rate-limiting only Internet Group Management Protocol (IGMP) control packets. For Layer 3 packets, on a port in nonrouting mode (whether or not a Layer 2 service policy is attached), only IP packets with router MAC addresses are dropped.

These types of control packets are dropped or rate-limited:

- Layer 2 protocol control packets:
  - Control packets that are always dropped on UNIs and ENIs, such as Dynamic Trunking Protocol (DTP) packets and some bridge protocol data units (BPDUs).
  - Control packets that are dropped by default but can be enabled or tunneled, such as CDP, STP, LLDP, VLAN Trunking Protocol (VTP), UniDirectional Link Detection (UDLD) Protocol, LACP, and PAgP packets. When enabled, these protocol packets are rate-limited and tunneled through the switch.
  - Control or management packets that are required by the switch, such as keepalive packets. These control packets are processed by the CPU but are rate-limited to normal and safe limits to prevent CPU overload.
- Non-IP packets with router MAC addresses
- IP packets with router MAC addresses
- IGMP control packets that are enabled by default and need to be rate-limited. However, when IGMP snooping and IP multicast routing are disabled, the packets are treated like data packets, and no policers are assigned to them.

The switch uses policing to accomplish control-plane security by either dropping or rate-limiting Layer 2 control packets. If a Layer 2 protocol is enabled on a UNI or ENI port or tunneled on the switch, those protocol packets are rate-limited; otherwise control packets are dropped.

By default, some protocol traffic is dropped by the CPU, and some is rate-limited. Table 35-1 shows the default action and the action taken for Layer 2 protocol packets when the feature is enabled or when Layer 2 protocol tunneling is enabled for the protocol. Note that some features cannot be enabled on UNIs, and not all protocols can be tunneled (shown by dashes). If Layer 2 protocol tunneling is enabled for *any* of the supported protocols (CDP, STP, VTP, LLDP, LACP, PAgP, or UDLD), the switch Layer 2 protocol tunneling protocol uses the rate-limiting policer on every port. If UDLD is enabled on a port or UDLD tunneling is enabled, UDLD packets are rate-limited.

Table 35-1 Control-Plane Security Actions on Layer 2 Protocol Packets Received on a UNI or ENI

Protocol	Default	When Feature Is Enabled	When Layer 2 Protocol Tunneling Is Enabled [1]
STP	Dropped	Rate limited **Note** STP can be enabled only on ENIs.	Rate-limited
RSVD_STP (reserved IEEE 802.1D addresses)	Dropped	When the Ethernet Link Management Interface (ELMI) is enabled, globally or on a per-port basis whichever is configured last, a throttle policer is assigned to a port. When ELMI is disabled (globally or on a port, whichever is configured last), a drop policer is assigned to a port.	–
PVST+	Dropped	–	Rate limited
LACP	Dropped	Rate limited **Note** LACP can be enabled only on ENIs.	Rate limited
PAgP	Dropped	Rate limited **Note** PAgP can be enabled only on ENIs.	Rate limited
IEEE 802.1x	Dropped	Rate limited	–
CDP	Dropped	Rate limited **Note** CDP can be enabled only on ENIs.	Rate limited
LLDP	Dropped	Rate limited **Note** LLDP can be enabled only on ENIs.	Rate limited
DTP	Dropped	–	–
UDLD	Dropped	Rate limited	Rate limited
VTP	Dropped	–	Rate limited
CISCO_L2 (any other Cisco Layer 2 protocols with the MAC address 01:00:0c:cc:cc:cc)	Dropped	–	Rate limited if CDP, DTP, UDLD, PAGP, or VTP are Layer 2 tunneled
KEEPALIVE (MAC address, SNAP encapsulation, LLC, Org ID, or HDLC packets)	Rate-limited	–	–

1. Layer 2 protocol traffic is rate-limited when Layer 2 protocol tunneling is enabled for any protocol on any port.

The switch automatically allocates 27 control-plane security policers for CPU protection. At system bootup, it assigns a policer to each port numbered 0 to 26. The policer assigned to a port determines if the protocol packets arriving on the port are rate-limited or dropped. On the CGS 2520 switch, a policer of 26 means a drop policer and is a global policer; any traffic type shown as 26 on any port is dropped. A policer of a value of 0 to 25 means that a rate-limiting policer is assigned to the port for the protocol. The policers 0 to 23 are logical identifiers for Fast Ethernet ports 1 to 24; policers 24 and 25 refer to Gigabit Ethernet ports 1 and 2, respectively. A policer value of 255 means that no policer is assigned to a protocol.

To see what policer actions are assigned to the protocols on an interface, enter the **show platform policer cpu interface** *interface-id* privileged EXEC command.

This example shows the default policer configuration for a UNI. Because the port is Fast Ethernet 1, the identifier for rate-limited protocols is 0; a display for Fast Ethernet port 5 would display an identifier of 4. The *Policer Index* refers to the specific protocol. The ASIC number shows when the policer is on a different ASIC.

Because UNIs do not support STP, CDP, LLDP, LACP, and PAgP, these packets are dropped (physical policer of 26). These protocols are disabled by default on ENIs as well, but you can enable them. When enabled on ENIs, the control packets are rate limited and a rate-limiting policer is assigned to the port for these protocols (physical policer of 22).

```
Switch# show platform policer cpu interface fastethernet 0/3
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/1
STP                                 1             26             0
LACP                                2             26             0
8021X                               3             26             0
RSVD_STP                            4             26             0
PVST_PLUS                           5             26             0
CDP                                 6             26             0
LLDP                                7             26             0
DTP                                 8             26             0
UDLD                                9             26             0
PAGP                               10             26             0
VTP                                11             26             0
CISCO_L2                           12             26             0
KEEPALIVE                          13              0             0
CFM                                14            255             0
SWITCH_MAC                         15             26             0
SWITCH_ROUTER_MAC                  16             26             0
SWITCH_IGMP                        17              0             0
SWITCH_L2PT                        18             26             0
```

This example shows the policers assigned to a ENI when control protocols are enabled on the interface. A value of 22 shows that protocol packets are rate limited for that protocol. When the protocol is not enabled, the defaults are the same as for a UNI.

```
Switch# show platform policer cpu interface fastethernet0/23
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/23
STP                                 1             26             0
LACP                                2             22             0
8021X                               3             26             0
RSVD_STP                            4             26             0
PVST_PLUS                           5             26             0
CDP                                 6             22             0
LLDP                                7             26             0
DTP                                 8             26             0
UDLD                                9             26             0
PAGP                               10             26             0
VTP                                11             26             0
CISCO_L2                           12             22             0
KEEPALIVE                          13             22             0
```

```
CFM                                14          255            0
SWITCH_MAC                         15           26            0
SWITCH_ROUTER_MAC                  16           26            0
SWITCH_IGMP                        17           22            0
SWITCH_L2PT                        18           22            0
```

This example shows the default policers assigned to NNIs. Most protocols have no policers assigned to NNIs. A value of 255 means that no policer is assigned to the port for the protocol.

```
Switch #show platform policer cpu interface gigabitethernet 0/1
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Gi0/1
STP                                 1           255            0
LACP                                2           255            0
8021X                               3           255            0
RSVD_STP                            4           255            0
PVST_PLUS                           5           255            0
CDP                                 6           255            0
LLDP                                7           255            0
DTP                                 8           255            0
UDLD                                9           255            0
PAGP                               10           255            0
VTP                                11           255            0
CISCO_L2                           12           255            0
KEEPALIVE                          13           255            0
CFM                                14           255            0
SWITCH_MAC                         15           255            0
SWITCH_ROUTER_MAC                  16           255            0
SWITCH_IGMP                        17           255            0
SWITCH_L2PT                        18           255            0
```

Configuring Control-Plane Security

CPU protection is enabled by default and CPU policers are pre-allocated. You can disable CPU protection by entering the **no policer cpu uni all** global configuration command or reenable it by entering the **policer cpu uni all** global configuration command. When you disable or enable CPU protection, you must reload the switch by entering the **reload** privileged EXEC command before the configuration takes effect.

When CPU protection is enabled, you can configure only 45 policers per port. Disabling CPU protection allows you to configure up to 64 policers per port. Note these limitations when you disable CPU protection:

- When CPU protection is disabled, you can configure a maximum of 63 policers per port for user-defined classes and one for class-default.
- Due to hardware limitations, you can attach 64 per-port, per-VLAN policers to a maximum of 6 ports. If you attempt to attach more than 6 per-port per VLAN 64-policer policy maps, the attachment fails with a *VLAN labels exceeded* error message.
- If you disable CPU protection and attach a policy map with more than 45 policers, and then enable CPU protection again, and reload, 19 policers per port are again required for CPU protection. During reload, the policers 46 and above will reach the *policer resources exceeded* error condition and no policers are attached to those classes.

You can configure only the rate-limiting threshold. The configured threshold applies to all supported control protocols on all UNIs and ENIs. It also applies to STP, CDP, LLDP, LACP, and PAgP when the protocol is enabled on an ENI.

Note During normal Layer 2 operation, you cannot ping the switch through a UNI or ENI. This restriction does not apply to NNIs. See the "Using Ping" section on page 48-8 for ways to enable ping in a test situation.

Beginning in privileged EXEC mode, follow these steps to set the threshold rate for CPU protection:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**policer cpu uni** *rate*	Configure the CPU protection policing threshold rate. The range is from 8000 to 409500 bits per second (b/s). The default, if none is configured, is 160000 b/s. **Note** The configured rate applies to all supported and enabled control protocols on all UNIs and ENIs
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show policer cpu uni-eni rate**	Verify the configured CPU policer rate.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default threshold rate, use the **no policer cpu uni** global configuration command. To disable CPU protection, enter the **no policer cpu uni all** global configuration command, and reload the switch.

This example shows how to set the CPU protection threshold to 10000 b/s and to verify the configuration.

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# policer cpu uni 10000
Switch(config)# end
Switch# show policer cpu uni-eni rate
CPU UNI/ENI port police rate = 10000 bps
```

This is an example of the show command output when CPU protection is disabled.

```
Switch# show policer cpu uni-eni rate
CPU Protection feature is not enabled
```

Monitoring Control-Plane Security

You can monitor control-plane security settings and statistics on the switch or on an interface, and you can clear these statistics at any time by using the privileged EXEC commands in Table 35-2. For more information about the commands, see the command reference for this release.

Table 35-2 Commands for Monitoring Control-Plane Security

Command	Purpose
clear policer cpu uni-eni counters {**classification** | **drop**}	Clear all control-plane statistics per feature (**classification**) or all statistics maintained by the control-plane policer (**drop**).
debug platform policer cpu uni-eni	Enable debugging of the control-plane policer. This command displays information messages when any changes are made to CPU protection.
show platform policer cpu {**classification** | **interface** *interface-id*}	Display control-plane policer information. • **classification**—show classification statistics. • **interface** *interface-id*—show policer indexes for the specified interface.

show policer cpu uni-eni {**drop** [**interface** *interface-id*] | **rate**}	Display CPU policer information for the switch.
	• **drop** [**interface** *interface-id*] —show the number of dropped frames for all interfaces or the specified interface.
	• **rate**—show the configured threshold rate for CPU policers.
	If CPU protection is disabled, this message appears in the output:
	`Switch# show policer cpu uni drop`
	`CPU Protection feature is not enabled`