CHAPTER 33

Configuring Control-Plane Security

This chapter describes the control-plane security feature in the Cisco ME 3400E Ethernet Access switch. In any network, Layer 2 and Layer 3 switches exchange control packets with other switches in the network. The Cisco ME 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.

This chapter includes these sections;

Understanding Control-Plane Security

In the Cisco ME 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 ME 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 ME 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.

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** 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

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:
  -
  -
  -

  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 33-1 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*

Table 33-1 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]
		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

Control-Plane Security Actions on Layer 2 Protocol Packets Received on a UNI or ENI (continued)

LACP	Dropped	Rate limited LACP can be enabled only on ENIs.	Rate limited
PAgP	Dropped	Rate limited PAgP can be enabled only on ENIs.	Rate limited
IEEE 802.1x	Dropped	Rate limited	–
CDP	Dropped	Rate limited CDP can be enabled only on ENIs.	Rate limited
LLDP	Dropped	Rate limited 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	–	–
Ethernet Connectivity Fault Management (CFM)	No policer assigned	When CFM is enabled globally, a throttle policer is assigned to all ports. When CFM is disabled globally, a NULL policer is assigned to all ports.	–

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 ME 3400E-24TS 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.

For the ME 3400EG-12CS and ME 34000EG-2CS switches, a policer of 4 means a drop policer. A traffic type shown as 4 on a port is dropped. A policer value of 0 to 3 means that a rate-limiting policer is assigned to the port for the 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.

Unless otherwise indicated, the examples are for an ME 3400E-24TS switch.

Policer Index

```
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
```

```
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
```

```
Switch #show platform policer cpu interface gigabitethernet 0/2
```

show platform policer cpu interface gigabitethernet 0/1

Configuring Control-Plane Security

Note

"Using Ping" section on page 43-10 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**	
Step 2	**policer cpu uni**	from 8000 to 409500 bits per second (b/s). The default, if none is configured, is 160000 b/s. 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 global configuration command.

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

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

Monitoring Control-Plane Security

Commands for Monitoring Control-Plane Security

Command	Purpose
clear policer cpu uni-eni counters {**classification** | **drop**}	Clears all control-plane statistics per feature (**classification**) or all statistics maintained by the control-plane policer (**drop**).
debug platform policer cpu uni-eni	Enables debugging of the control-plane policer. This command displays information messages when any changes are made to CPU protection.

Table 33-2 Commands for Monitoring Control-Plane Security (continued)

Command	Purpose
{ | }	Displays control-plane policer information. • —show classification statistics. • —show policer indexes for the specified interface.
show policer cpu uni-eni {**drop** [**interface** *interface-id*] | **rate**}	Displays CPU policer information for the switch. • [**interface** *interface-id*] —show the number of dropped frames for all interfaces or the specified interface. • —show the configured threshold rate for CPU policers. If CPU protection is disabled, this appears in the output for the command: