Quality of Service

This chapter describes how to identify and resolve problems related to Quality of Service (QoS).

Information About Quality of Service

QoS allows you to classify network traffic so that it can be policed and prioritized in a way that prevents congestion. Traffic is processed based on how you classify it and the QoS policies that you put in place. Classification, marking, and policing are the three main features of QoS.

- Traffic Classification—Groups network traffic based on defined criteria.
- Traffic Marking—Modifies traffic attributes such as DSCP, class of service (CoS), and precedence by class.
- Policing—Monitors data rates and burst sizes for a particular class of traffic. QoS policing on a network determines whether network traffic is within a specified profile (contract).

For detailed information about QoS, see the *Cisco Nexus 1000V for Microsoft Hyper-V Quality of Service Configuration Guide*.

QoS Configuration Limits

Table 16-1 and Table 16-2 list the configuration limits for QoS.

Table 16-1 QoS Configuration Limits

Item	DVS Limit	Per Server Limit
Class map	1000	64 (with policies)
Policy map	128	16
Service policy	—	128

Table 16-2 QoS Configuration Limits

Item	Limit
Match criteria per class map	32
Class maps per policy map	64

QoS VSM Troubleshooting Commands

You can use the commands in this section on the Virtual Supervisor Module (VSM) to troubleshoot the policies that are configured and applied on the interfaces.

Display configured policies and class maps by entering these commands:

- **show policy-map** [*policy-map-name*]
- **show class-map** [*class-map-name*]

Display installed policies by entering this command:

- **show policy-map interface brief**

Collect QOSMGR process run-time information configuration errors by entering these commands on the VSM:

- **show system internal ipqos event-history errors**
- **show system internal ipqos event-history msgs**
- **show system internal ipqos port-node**
- **show system internal ipqos mem-stats** (to debug memory usage and leaks)
- **show system internal ipqos status**
- **show system internal ipqos log** (to show aborted plan information)
- **show system internal ipqos**

Collect ACLCOMP process run-time information configuration errors by entering these commands on the VSM:

- **show system internal aclcomp event-history errors**
- **show system internal aclcomp event-history msgs**
- **show system internal aclcomp pdl detailed**
- **show system internal aclcomp mem-stats** (to debug memory usage and leaks)

QoS VEM Troubleshooting Commands

You can use the commands in this section to display configured QoS policies on the VEM.

To list all class maps and policies in use on the server, enter this command:

- **module vem** *module-number* **execute vemcmd show qos node #**

```
n1000v# module vem 3 execute vemcmd show qos node
nodeid   type     details
-------- -------- --------
```

```
0   policer
           cir:50 pir:50
           bc:200000 be:200000
           cir/pir units 1 bc/be units 3 flags 2
1    class   op_AND
              DSCP
2    class op_DEFAULT
```

To list all the installed policy maps in use on the server, enter this command:

- **module vem** *module-number* **execute vemcmd show qos policy**

```
n1000v# module vem 3 execute vemcmd show qos policy
policyid classid policerid set_type value
-------- -------- -------- -------- --------
       0        1       -1             dscp        5
                2        0              dscp        0
```

To list all service policies installed on the server, enter this command:

- **module vem** *module-number* **execute vemcmd show qos pinst**

```
n1000v# module vem 3 execute vemcmd show qos pinst


id       type
-------- --------
      17  Ingress
            class        bytes matched         pkts matched
           -------- -------------------- --------------------
                  1                    0                    0

                  2                85529                  572
                  0
                    policer stats: conforming (85529, 572)
                    policer stats: exceeding (0, 0)
                    policer stats: violating (0, 0)
```

Debugging Policing Verification Errors

Step 1 Enter the **debug aclmgr all** command if the policy references an ACL.

Step 2 Set all debug flags for IP QoS manager by entering the **debug ipqos all** command.

Step 3 Configure all aclcomp debug flags by entering the **debug aclcomp all** command.

Step 4 Execute the command once again with debug traces output to the console by entering the **service-policy** command. This command allows you to collect logs for all operations.

Step 5 Save the Telnet SSH session buffer to a file.

If you are debugging a policy on a port profile, it might be easier to first install it directly on an interface.

Step 1 Clear the log by entering the **module vem** *module-number* **execute vemcmd dpa clear** command.

Step 2 Redirect the output of the dpa logs to the vemlog by entering the **module vem** *module-number* **execute vemcmd dpa sfqosagent all** command.

Step 3 Start the vecmd DPA by entering the **module vem** *module-number* **execute vemcmd dpa start** command.

Step 4 Execute the command once again with the DPA debug traces output to vemcmd dpa by entering the **service-policy** command.

Step 5 Stop the vemcmd DPA by entering the **module vem** *module-number* **execute vemcmd dpa stop** command.

Step 6 See the logs on the console by entering the **module vem** *module-number* **execute vemlog show all** command.

The output looks similar to the following:

```
calling add policy 81610ac len 220 classmaps 3- --> Session actions
…
Adding classmap 1 (108) with op 1 and 2 filters
…
Adding classmap 2 (116) with op 2 and 2 filters
…
Adding classmap 3 (56) with op 0 and 0 filters
…
init pinst ltl 11 policy id 0 if_index 1a020200 --> Service-policy being applied
installing pinst type 0 17 for policy 0
dpa_sf_qos_verify returned 0
…
Session commit complete and successful --> Session ending
```