CHAPTER 11

Quality of Service

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

This chapter includes the following sections:

- Information About Quality of Service, page 11-1
- QoS Configuration Limits, page 11-1
- QoS Troubleshooting Commands, page 11-2
- Troubleshooting the VEM, page 11-2
- Debugging Policing Verification Errors, page 11-3

Information About Quality of Service

QoS lets you 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, 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, refer to the *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)*.

QoS Configuration Limits

Table 11-1 land Table 11-2 list the configuration limits for QoS.

Table 11-1 QoS Configuration Limits

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

Table 11-2 QoS Configuration Limits

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

QoS Troubleshooting Commands

The commands listed in this section can be used on the VSM to see the policies that are configured and applied on the interfaces.

Use the following commands to display configured policies and class-maps:

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

Use the following command to display installed policies:

- **Show policy-map interface brief**

Use following commands on the VSM to see run-time information of the QOSMGR and ACLCOMP during configuration errors.

The commands to collect QOSMGR process run-time information configuration errors are as follows:

- **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**

The commands to collect ACLCOMP process run-time information configuration errors are as follows:

- **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)

Troubleshooting the VEM

The commands listed in this section can be used to display configured QoS policies on the VEM.

Use the following command to list all class maps and polices in use on the server:

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

```
~ # 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
```

Use the following command to list all the installed policy maps in use on the server:

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

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

Use the following command to list all service policies installed on the server:

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

```
~ # 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

To debug a policy verification failure caused by processing on the VSM, follow these steps:

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

Step 2 Enter **debug ipqos all** command.

Step 3 Enter the **debug aclcomp all** command.

Step 4 Enter the **service-policy** command which will execute the command once again with debug traces output to the console. 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 may be easier to first install it directly on an interface.

To debug a policy verification failure on the VEM, follow these steps:

Step 1 Enter the **module vem** *module-number* **execute vemdpalog clear** command.

Step 2 Enter the **module vem** *module-number* **execute vemdpalog sfqosagent all** command.

Step 3 Enter **module vem** *module-number* **execute vemdpalog start** command.

Step 4 Enter the **service-policy** command which will execute the command once again with the DPA debug traces output to vemdpalog.

Step 5 Enter **module vem** *module-number* **execute vemdpalog stop** command.

Step 6 Enter the **module vem** *module-number* **execute vemdpalog show all** command to see the logs on console.

The output will look 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
```