

# Monitoring Resources

---

## Contents

<b>Viewing Information on Resource Usage</b> .....	E-2
Policy Enforcement Engine .....	E-2
Displaying Current Resource Usage .....	E-4
<b>When Insufficient Resources Are Available</b> .....	E-7

## Viewing Information on Resource Usage

The switch allows you to view information about the current usage and availability of resources in the Policy Enforcement engine, including the following software features:

- Access control lists (ACL)
- Quality-of-service (QoS), including device and application port priority, ICMP rate-limiting, and QoS policies
- Dynamic assignment of per-port or per-user ACLs and QoS through RADIUS authentication designated as “IDM”, with or without the optional identity-driven management (IDM) application
- Virus throttling (VT) using connection-rate filtering
- Mirroring policies, including switch configuration as an endpoint for remote intelligent mirroring
- Other features, including:
  - Management VLAN
  - DHCP snooping
  - Dynamic ARP protection
  - Jumbo IP-MTU

## Policy Enforcement Engine

The Policy Enforcement engine is the hardware element in the switch that manages quality-of-service, mirroring, and ACL policies as well as other software features, using the rules that you configure. Resource usage in the Policy Enforcement engine is based on how these features are configured on the switch.

- Resource usage by dynamic port ACLs and virus-throttling is determined as follows:
  - Dynamic port ACLs configured by a RADIUS server (with or without the optional IDM application) for an authenticated client determine the current resource consumption for this feature on a specified slot. When a client session ends, the resources in use for that client become available for other uses.
  - A virus-throttling configuration (connection-rate filtering) on the switch does not affect switch resources unless traffic behavior has triggered either a throttling or blocking action on the traffic from one or more clients. When the throttling action ceases or a blocked client is unblocked, the resources used for that action are released.

- When the following features are configured globally or per-VLAN, resource usage is applied across all port groups or all slots with installed modules:
  - ACLs
  - QoS configurations that use the following commands:
    - QoS device priority (IP Address) through the CLI using the **qos device-priority** command
    - QoS application port through the CLI using **qos tcp-port** or **qos udp-port**
    - VLAN QoS Policies through the CLI using **service-policy**
  - Management VLAN configuration
  - DHCP snooping
  - Dynamic ARP protection
  - Remote mirroring endpoint configuration
  - Mirror policies per VLAN through the CLI using **monitor service**
  - Jumbo IP-MTU
- When the following features are configured per-port, resource usage is applied only to the slot or port group on which the feature is configured:
  - ACLs or QoS applied per-port or per-user through RADIUS authentication
  - ACLs applied per-port through the CLI using the **ip access-group** or **ipv6 traffic-filter** commands
  - QoS policies applied per port through the CLI using the **service-policy** command
  - Mirror policies applied per-port through the CLI using the **monitor all service** and **service-policy** commands
  - ICMP rate-limiting through the CLI using the **rate-limit icmp** command
  - Virus throttling applied to any port (when a high connection-rate client is being throttled or blocked)

## Displaying Current Resource Usage

To display current resource usage in the switch, enter the **show** <qos | access-list | policy> **resources** command.

The **show resources** command output allows you to view current resource usage and, if necessary, prioritize and reconfigure software features to free resources reserved for less important features.

The **qos**, **access-list**, and **policy** parameters display the same command output and provide different ways to access task-specific information.

**Syntax:** show <qos | access-list | policy> resources

*Displays the resource usage of the Policy Enforcement Engine on the switch by software feature. For each type of resource, the amount still available and the amount used by each software feature is shown.*

Figure E1 shows the resource usage on a 3500y1 switch configured for ACLs, QoS, RADIUS-based authentication, and other features:

- The “Rules Used” columns show that ACLs, virus-throttling (VT), mirroring, and other features (for example, Management VLAN) have been configured globally or per-VLAN because identical resource consumption is displayed for each port range in the switch. If ACLs were configured per-port, the number of rules used in each port range would be different.
- The switch is also configured for virus throttling, and is either blocking or throttling routed traffic with a high rate of connection requests.
- Varying ICMP rate-limiting configurations on ports 1-24, on ports 25-48, and on slot A, have resulted in different meter usage and different rule usage listed under QoS. Global QoS settings would otherwise result in identical resource consumption on each port range in the switch.
- There is authenticated client usage of IDM resources on ports 25-48.

```

ProCurve# show qos resources

Resource usage in Policy Enforcement Engine

  Ports |      Rules      | Rules Used
  -----+-----+-----+-----+-----+-----+-----+-----+-----
  Ports | Available | ACL | QoS | IDM | VT | Mirror | Other |
  -----+-----+-----+-----+-----+-----+-----+-----+-----
  1-24 |      3014 |   15 |   11 |   0 |   1 |   0 |   3 |
  25-48 |      3005 |   15 |   10 |   10 |   1 |   0 |   3 |
  A     |      3017 |   15 |    8 |    0 |   1 |   0 |   3 |

  Ports |      Meters      | Meters Used
  -----+-----+-----+-----+-----+-----+-----+-----+-----
  Ports | Available | ACL | QoS | IDM | VT | Mirror | Other |
  -----+-----+-----+-----+-----+-----+-----+-----+-----
  1-24 |      250 |    |    5 |    0 |    |    |    0 |
  25-48 |      251 |    |    4 |    0 |    |    |    0 |
  A     |      253 |    |    2 |    0 |    |    |    0 |

  Ports | Application | Application Port Ranges Used
  -----+-----+-----+-----+-----+-----+-----+-----+-----
  Ports | Available | ACL | QoS | IDM | VT | Mirror | Other |
  -----+-----+-----+-----+-----+-----+-----+-----+-----
  1-24 |      3014 |   2 |   0 |   0 |    |    0 |   0 |
  25-48 |      3005 |   2 |   0 |   0 |    |    0 |   0 |
  A     |      3017 |   2 |   0 |   0 |    |    0 |   0 |

0 of 8 Policy Engine management resources used.
Key:
ACL = Access Control Lists
QoS = Device & Application Port Priority, QoS Policies, ICMP rate limits
IDM = Identity Driven Management
VT = Virus Throttling blocks
Mirror = Mirror Policies, Remote Intelligent Mirror endpoints
Other = Management VLAN, DHCP Snooping, ARP Protection, Jumbo IP-MTU.

Resource usage includes resources actually in use, or reserved for future
use by the listed feature. Internal dedicated-purpose resources, such as
port bandwidth limits or VLAN QoS priority, are not included.

```

**Figure E1. Example of Displaying Current Resource Usage on a Series 3500yl Switch**

---

#### Usage Notes for show resources Output

- A 1:1 mapping of internal rules to configured policies in the switch does not necessarily exist. As a result, displaying current resource usage is the most reliable method for keeping track of available resources. Also, because some internal resources are used by multiple features, deleting a feature configuration may not increase the amount of available resources.
  - Resource usage includes resources actually in use or reserved for future use by the listed features.
  - “Internal dedicated-purpose resources” include the following features:
    - Per-port ingress and egress rate limiting through the CLI using **rate-limit in/out**
    - Per-port ingress and egress broadcast rate limiting through the CLI using **rate-limit bcast/mcast**
    - Per-port or per-vlan priority or DSCP through the CLI using **qos priority** or **qos dscp**
    - Per protocol priority through the CLI using **qos protocol**
  - For chassis products (for example, the 5400zl or 8212zl switches), ‘slots’ are listed instead of ‘ports’ with resources shown for all installed modules on the chassis.
  - The “Available” columns display the resources available for additional feature use.
  - The “IDM” column shows the resources used for RADIUS-based authentication with or without the IDM option.
  - “Meters” are used when applying either ICMP rate-limiting or a QoS policy with a rate-limit class action.
-

## When Insufficient Resources Are Available

The switch has ample resources for configuring features and supporting:

- RADIUS-authenticated clients (with or without the optional IDM application)
- Virus throttling and blocking on individual clients.

---

### **Note**

---

Virus throttling does not operate on IPv6 traffic.

If the resources supporting these features become fully subscribed:

- The current feature configuration, RADIUS-authenticated client sessions, and virus throttling instances continue to operate normally.
- The switch generates an event log notice to say that current resources are fully subscribed.
- Currently engaged resources must be released before any of the following actions are supported:
  - Modifying currently configured ACLs, IDM, virus throttling, and other software features, such as Management VLAN, DHCP snooping, and dynamic ARP protection.

You can modify currently configured classifier-base QoS and mirroring policies if a policy has not been applied to an interface. However, sufficient resources must be available when you apply a configured policy to an interface.

- Acceptance of new RADIUS-based client authentication requests (displayed as a new resource entry for IDM).

Failure to authenticate a client that presents valid credentials may indicate that insufficient resources are available for the features configured for the client in the RADIUS server. To troubleshoot, check the event log.

- Throttling or blocking of newly detected clients with a high rate of connection requests (as defined by the current virus-throttling configuration).

The switch continues to generate event log notifications (and SNMP trap notification, if configured) for new instances of high connection-rate behavior detected by the virus-throttling feature.

**Monitoring Resources**  
When Insufficient Resources Are Available