Monitoring Resources

Contents

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 (ACLs)
- Quality-of-service (QoS) policies
- Dynamic assignment of port-based ACLs through RADIUS authentication, with or without the optional identity-driven management (IDM) application
- Virus throttling (using connection-rate filtering)
- ICMP rate-limiting
- Management VLAN
- DHCP snooping
- Dynamic ARP protection
- Switch configuration as an endpoint for remote mirroring

Policy Enforcement Engine

The Policy Enforcement engine is the hardware element in the switch that manages quality-of-service 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.

Resource usage by the following features, which are configured globally or per-VLAN, applies across all slots with installed modules:

- ACLs

- QoS configurations
- Management VLAN configuration
- DHCP snooping
- Dynamic ARP protection
- Remote-mirroring endpoint configuration

Resource usage on the following features, which are configured per-port, applies only to the slot or port group on which the feature is configured:

- ACLs applied per-port through RADIUS authentication
- ACLs applied per-port through the CLI using the **ip access-group** and **monitor ip** commands.
- ICMP rate-limiting
- 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 resources** command.

Syntax: show <qos | access-list> 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.

The **qos** *and* **access-list** *parameters display the same command output.*

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

Note

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.

Figure E1 shows the resource usage on a 3500yl switch configured for ACLs, QoS, RADIUS-based authentication, ICMP, and other features. Note that the switch is also configured for virus throttling and is either blocking or throttling routed traffic with a high rate of connection requests.

In this example, the "Rules Available" column displays the resources available for additional feature use. The "Rules Used" columns show that configured ACL, QoS, and other (for example, Management VLAN) resources, as well as the current blocking or throttling of a client by the virus-throttling (VT) feature, all result in identical resource consumption on each port range in the switch. At the same time, there is authenticated client usage of IDM resources on ports 25-48, and ICMP rate-limiting usage of different resource levels on ports 1-24 and 25-48, and on slot A. The "IDM" column shows the rules used for RADIUS-based authentication with or without the IDM option.

```
ProCurve# show access-list resources

 Resource usage in Policy Enforcement Engine

        |   Rules    |                Rules Used
  Ports | Available | ACL   | QoS   | IDM   |  VT   | ICMP | Other |
  ------+-----------+------+------+------+------+------+-------+
  1-24  |      3014 |   15 |    6 |    0 |    1 |    5 |     3 |
  25-48 |      3005 |   15 |    6 |   10 |    1 |    4 |     3 |
  A     |      3017 |   15 |    6 |    0 |    1 |    2 |     3 |

        | Application |    Application    |
        | Port Ranges | Port Ranges Used  |
  Ports |  Available* |   ACL    |   IDM    |
  ------+-------------+---------+---------+
  1-24  |          14 |       2 |       0 |
  25-48 |          14 |       2 |       0 |
  A     |          14 |       2 |       0 |

 * If insufficient port ranges are available, additional rules will be used.

0 of 8 Policy Engine management resources used.

Key:
ACL = Access Control Lists;  QoS = Host or application port QoS policies;
IDM = Identity Driven Management; VT = Virus Throttling;
ICMP = network ICMP rate limiting;
Other = Management VLAN, Remote Intelligent Mirror endpoints, DHCP Protection.

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 policies, are not included.
```

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

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

If virus throttling is enabled on a port and a large amount of IPv6 traffic goes through that port, the CPU resources may be used up. ProCurve recommends that you do not enable virus throttling on any port that may receive large amounts of 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:
  - Configuration of new entries for QoS, ACLs, virus throttling, ICMP rate-limiting, Management VLAN, DHCP snooping, dynamic ARP protection, and remote-mirroring endpoint features.
  - Acceptance of new RADIUS-based client authentication requests.

Note

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.