**mls rate-limit unicast ip**

To enable and set the rate limiters for the unicast packets, use the `mls rate-limit unicast ip` command. Use the `no` form of this command to disable the rate limiters.

```
mls rate-limit unicast ip {arp-inspection | dhcp-snooping | errors | features | options | rpf-failure} pps [packets-in-burst]
mls rate-limit unicast ip icmp {redirect | unreachable {acl-drop pps} | no-route pps} [packets-in-burst]
no mls rate-limit unicast ip {errors | features | {icmp {redirect | unreachable {acl-drop | no-route}}}} | options | rpf-failure} pps [packets-in-burst]
```

### Syntax Description

- **arp-inspection**: Specifies rate limiting for unicast packets with Dynamic Arp Inspection (DAI).
- **dhcp-snooping**: Specifies two independent rate limiters for unicast packets with Dynamic Host Configuration Protocol (DHCP). Because the two rate limiters are independent, it is not possible to limit all aggregate DHCP traffic with a single rate. Either divide the aggregate rate in half or allow both directions to use the full bandwidth simultaneously.
- **errors**: Specifies rate limiting for unicast packets with IP checksum and length errors.
- **features**: Specifies rate limiting for unicast packets with software-security features in Layer 3 (for example, authorization proxy, IPsec, and inspection).
- **options**: Specifies rate limiting for unicast IPv4 packets with options.
- **rpf-failure**: Specifies rate limiting for unicast packets with RPF failures.
- **pps**: Packets per second; see the “Usage Guidelines” section for valid values.
- **packets-in-burst**: (Optional) Packets in burst; valid values are from 1 to 255.
- **icmp redirect**: Specifies rate limiting for unicast packets requiring ICMP redirect.
- **icmp unreachable acl-drop pps**: Enables and sets the rate limiters for the ICMP unreachables for the ACL-dropped packets.
- **icmp unreachable no-route pps**: Enables and sets the rate limiters for the ICMP unreachables for the FIB-miss packets.

### Defaults

The defaults are as follows:

- If the `packets-in-burst` is not set, a default of 10 is programmed as the burst for unicast cases.
- **arp-inspection**—Enabled at 500 pps and `packets-in-burst` set to 10.
- **dhcp-snooping**—Enabled at 500 pps and `packets-in-burst` set to 10.
- **errors**—Enabled at 500 pps and `packets-in-burst` set to 10.
- **rpf-failure**—Enabled at 500 pps and `packets-in-burst` set to 10.
- **icmp unreachable acl-drop**—Enabled at 500 pps and `packets-in-burst` set to 10.
- **icmp unreachable no-route**—Enabled at 500 pps and `packets-in-burst` set to 10.
- **icmp redirect**—Disabled.
Command Modes

- Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17a)SX</td>
<td>The mls rate-limit unicast command added the ip keyword to the following:</td>
</tr>
<tr>
<td></td>
<td>- options</td>
</tr>
<tr>
<td></td>
<td>- icmp</td>
</tr>
<tr>
<td></td>
<td>- rpf-failure</td>
</tr>
<tr>
<td></td>
<td>- errors</td>
</tr>
<tr>
<td></td>
<td>- features</td>
</tr>
<tr>
<td></td>
<td>These keywords were changed as follows:</td>
</tr>
<tr>
<td></td>
<td>- The features keyword replaced the 13-features keyword.</td>
</tr>
<tr>
<td></td>
<td>- The mls rate-limit unicast icmp-redirect command replaced the mls rate-</td>
</tr>
<tr>
<td></td>
<td>limit unicast icmp-redirect command.</td>
</tr>
<tr>
<td></td>
<td>- The mls rate-limit unicast icmp unreachable command replaced the mls</td>
</tr>
<tr>
<td></td>
<td>rate-limit unicast icmp-unreachable command.</td>
</tr>
<tr>
<td>12.2(33)ZW</td>
<td>The following keywords were added:</td>
</tr>
<tr>
<td></td>
<td>- arp-inspection</td>
</tr>
<tr>
<td></td>
<td>- dhcp-snooping</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

To provide OAL support for denied packets, enter the mls rate-limit unicast ip icmp unreachable acl-drop 0 command.

OAL and VACL capture are incompatible. Do not configure both features on the switch. With OAL configured, use SPAN to capture traffic.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

Note

When you configure an ICMP rate limiter, and an ICMP redirect occurs, exiting data traffic is dropped while the remaining traffic on the same interface is forwarded.

When setting the pps, the valid values are 0 and from 10 to 1000000. Setting the pps to 0 globally disables the redirection of the packets to the route processor. The 0 value is supported for these rate limiters:

- ICMP unreachable ACL-drop
- ICMP unreachable no-route
- ICMP redirect
Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- **Group 1:**
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- **Group 2:**
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to 0 (zero) for a particular case.
- When the ingress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

### Examples

This example shows how to set the ICMP-redirect limiter for unicast packets:

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mls rate-limit</code></td>
<td>Displays information about the MLS rate limiter.</td>
</tr>
</tbody>
</table>