

Verifying That MAC Limiting Is Working Correctly

MAC limiting protects against flooding of the Ethernet switching table. MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

JUNOS Software provides two MAC limiting methods:

- Maximum number of dynamic MAC addresses allowed per interface—When the limit is exceeded, incoming packets with new MAC addresses are dropped.
- Specific “allowed” MAC addresses for the access interface—Any MAC address that is not in the list of configured addresses is not learned.

To verify MAC limiting configurations:

1. Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly on page 1
2. Verifying That Allowed MAC Addresses Are Working Correctly on page 2
3. Verifying Results of Various Action Settings When the MAC Limit Is Exceeded on page 2
4. Customizing the Ethernet Switching Table Display to View Information for a Specific Interface on page 5

Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly

Purpose Verify that MAC limiting for dynamic MAC addresses is working on the switch.

Action Display the MAC addresses that have been learned. The following sample output shows the results when two packets were sent from hosts on `ge-0/0/1` and five packets requests were sent from hosts on `ge-0/0/2`, with both interfaces set to a MAC limit of 4 with the action `drop`:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 7 entries, 6 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	-	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:77	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:79	Learn	0	ge-0/0/1.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0

Meaning The sample output shows that with a MAC limit of 4 for each interface, the packet for a fifth MAC address on `ge-0/0/2` was dropped because it exceeded the MAC limit. The address was not learned, and thus an asterisk (*) rather than an address appears in the **MAC address** column in the first line of the sample output.

Verifying That Allowed MAC Addresses Are Working Correctly

Purpose Verify that allowed MAC addresses are working on the switch.

Action Display the MAC cache information after allowed MAC addresses have been configured on an interface. The following sample shows the MAC cache after 5 allowed MAC addresses had been configured on interface `ge-0/0/2`. In this instance, the interface was also set to a dynamic MAC limit of 4 with action `drop`.

```
user@switch> show ethernet-switching table
Ethernet-switching table: 5 entries, 4 learned
```

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	*	Flood	-	ge-0/0/2.0

Meaning Because the MAC limit value for this interface had been set to 4, only four of the five configured allowed addresses were learned and thus added to the MAC cache. Because the fifth address was not learned, an asterisk (*) rather than an address appears in the MAC address column in the last line of the sample output.

Verifying Results of Various Action Settings When the MAC Limit Is Exceeded

Purpose Verify the results provided by the various action settings for MAC limits—drop, log, none, and shutdown—when the limits are exceeded.

Action Display the results of the various action settings.



NOTE: You can view log messages by using the `show log messages` command. You can also have the log messages displayed by configuring the monitor start messages with the `monitor start messages` command.

- **drop action**—For MAC limiting configured with a **drop** action and with the MAC limit set to 5:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 6 entries, 5 learned

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	–	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:88	Learn	0	ge-0/0/2.0

- **log action**—For MAC limiting configured with a **log** action and with MAC limit set to 5:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 74 entries, 73 learned

VLAN	MAC address	Type	Age	Interfaces
employee-vlan	*	Flood	–	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:80	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:81	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:82	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:83	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:84	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:85	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:87	Learn	0	ge-0/0/2.0
employee-vlan	00:05:85:3A:82:88	Learn	0	ge-0/0/2.0
. . .				

- **shutdown action**—For MAC limiting configured with a **shutdown** action and with MAC limit set to 3:

```
user@switch> show ethernet-switching table
```

Ethernet-switching table: 4 entries, 3 learned					
VLAN	MAC address	Type	Age	Interfaces	
employee-vlan	*	Flood	-	ge-0/0/2.0	
employee-vlan	00:05:85:3A:82:82	Learn	0	ge-0/0/2.0	
employee-vlan	00:05:85:3A:82:84	Learn	0	ge-0/0/2.0	
employee-vlan	00:05:85:3A:82:87	Learn	0	ge-0/0/2.0	

- **none** action—If you set a MAC limit to apply to all interfaces on the switch, you can override that setting for a particular interface by specifying this action for that interface. See *Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure)*.

Meaning For the **drop** action results—The sixth MAC address exceeded the MAC limit. The request packet for that address was dropped. Only five MAC addresses have been learned on **ge-0/0/2**.

For the **log** action results—The sixth MAC address exceeded the MAC limit. No MAC addresses were blocked.

For the **shutdown** action results—The fourth MAC address exceeded the MAC limit. Only three MAC addresses have been learned on **ge-0/0/2**. The interface **ge-0/0/1** is shut down.

For more information about interfaces that have been shut down, use the **show ethernet-switching interfaces** command.

```

user@switch> show ethernet-switching interfaces
Interface    State  VLAN members      Tag  Tagging  Blocking

bme0.32770   down   mgmt               untagged unblocked
ge-1/0/0.0   down   v1                 untagged MAC limit exceeded
ge-1/0/1.0   up     v1                 untagged unblocked
ge-1/0/2.0   up     v1                 untagged unblocked
me0.0        up     mgmt               untagged unblocked

```



NOTE: You can configure the switch to recover automatically from this type of error condition by specifying the `port-error-disable` statement with a `disable timeout` value. The switch automatically restores the disabled interface to service when the disable timeout expires. The `port-error-disable` configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after `port-error-disable` has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the `clear ethernet-switching port-error` command.

Customizing the Ethernet Switching Table Display to View Information for a Specific Interface

Purpose You can use the `show ethernet-switching table` command to view information for a specific interface.

Action For example, to display the MAC addresses that have been learned on `ge-0/0/2` interface, type:

```
user@switch> show ethernet-switching table interface ge-0/0/2.0
Ethernet-switching table: 1 unicast entries
```

VLAN	MAC address	Type	Age	Interfaces
v1	*	Flood	-	All-members
v1	00:00:06:00:00:00	Learn	0	ge-2/0/0.0

Meaning The MAC limit value for `ge-0/0/2` had been set to 1, and the output shows that only one MAC address was learned and thus added to the MAC cache. An asterisk (*) rather than an address appears in the **MAC address** column in the first line of the sample output.

- Related Topics**
- Configuring MAC Limiting (CLI Procedure)
 - Configuring MAC Limiting (J-Web Procedure)
 - Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)
 - Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks
 - Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks
 - Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks
 - Monitoring Port Security

Published: 2009-07-27