



MAC Limiting

This document describes how to configure MAC limiting.

- [Information About Global MAC Address Limiting on Bridge Domain, on page 1](#)
- [Restrictions for MAC Limiting, on page 2](#)
- [Configuring MAC Limiting, on page 3](#)

Information About Global MAC Address Limiting on Bridge Domain

Table 1: Feature History

Feature Name	Release Information	Description
Mac Address Limiting Per Bridge Domain	Cisco IOS XE Bengaluru 17.4.1	This feature restricts the number of MAC addresses that the router learns in a bridge-domain on an EFP or trunk EFP to a specified number. Use the feature to enable warning and limit actions when a violation occurs.
MAC Entry Flooding Limiting	Cisco IOS XE Cupertino 17.8.1	This feature allows the user to disable unknown unicast flooding on a certain bdomain using the flood sub action. This flood sub action is initiated only when the limit action is configured and violation has occurred.

MAC address limiting per bridge-domain restricts the number of MAC addresses that the router learns in a bridge-domain on an EFP or trunk EFP to a specified number.



Note Use the `mac-address-table limit bdomain num maximum 0 action limit` command to disable mac-learning on bridge-domain.

When the total number of MAC addresses (dynamic MAC addresses) in a bridge-domain exceeds the maximum number, then the router takes a violation action. The router either restricts further learning on bridge-domain by itself with a syslog or just intimate the user through a syslog to take further action.

You can enable the following actions when violation occurs:

- **Warning**—The violation is logged as a syslog message and no further action is taken. There is one syslog message received, when the MAC count exceeds the configured limit (exceed notification) and no more syslog messages are received for the bridge-domain (bdomain) unless the violation is no longer valid (drop notification). When you select the warning action, the further learning of new MAC addresses and forwarding of traffic continue to happen irrespective of violation.
- **Limit**—When the Limit option is selected as an action for violation, the MAC learning on the bdomain is disabled when violation occurs. No new MAC addresses are learnt on the bdomain until the recovery mechanism gets started. Even though new MAC addresses are not learned but frames are still flooded in the system. If user needs to stop flooding, then a sub action flood can also be used along with limit action.



Note The threshold value must be 80% of the maximum value configured for the recovery mechanism.

- **Flood**—The flood sub action allows the user to disable unknown unicast flooding on a given bdomain. This flood sub action is initiated only when the limit action is configured and violation has occurred. Unknown unicast flooding is disabled only for the interval necessary to limit the entries. Using this option, improves the performance and the flooding is re-enabled when the total number of MAC entries are dropped below the threshold value.



Note **Warning** is the default action when no action is configured.

For the limit and warning actions, the recovery mechanism is initiated when the total MAC limit count drops to equal or below a threshold value. The threshold value is dependent on the maximum limit configured on bridge domain (the threshold value is 80% of the limit value). The recovery mechanism reverts the action taken during violation. For example, if the MAC address learning is disabled as a violation action, then it will be re-enabled.

If no maximum value or action option is specified through the **mac address-table limit bdomain id maximum num action** command, then the default action (warning) and a default maximum value of 500 is configured.



Note For a MAC limit of 0 with the action limit, limit flood, the violation action occurs when the user configures it irrespective of MAC address learning on the bridge domain. The recovery mechanism is to disable the feature through the **no mac address-table limit bdomain id** command.

Restrictions for MAC Limiting

MAC limiting is supported on the following interface types:

- You can apply MAC limiting only to bridge-domains.
- MAC limiting is supported for dynamic MAC addresses.
- With **limit** keyword, the router sends a syslog message and generates a trap. MAC learning is disabled on the bridge-domain. The flooding of frames with new MAC address continues. To disable flooding, use the **flood** keyword. Flooding resumes only after the total number of MAC entries drop below the threshold value (80%).
- The allowed MAC limit range is from 0 through 16000.
- You can enable the MAC limit feature up to a maximum of 1000 bridge domains.

Configuring MAC Limiting

Procedure

- Step 1** **configure terminal**
Enter global configuration mode.
- Step 2** **mac-address-table limit** *bdomain id maximum num action {warning | limit} [flood]*
Sets the specific limit and any optional actions to be imposed at the bridge-domain level.
The default **maximum** value is 500.
- Step 3** **end**
Return to privileged EXEC mode.
- Step 4** **show mac-address-table limit bdomain** *bdomain id*
Displays the information about the MAC-address table.
- Step 5** **copy running-config startup-config**
(Optional) Save your entries in the configuration file.
-

Example of Enabling Per-Bridge-Domain MAC Limiting

This example shows how to enable per-bridge-domain MAC limiting.

```
Router# enable
Router# configure terminal
Router(config)# mac-address-table limit bdomain 10 maximum 100 action limit flood
Router(config)# end
```

Verifying the MAC Limiting on Bridge Domain

Use the **show mac address-table limit** command to verify the information related to configured MAC limit per bridge domain.

This example shows how to display the information related to configured MAC limit per bridge domain.

```
Router#show mac address-table limit bdomain 10
  bdomain      action      flood      maximum      Total entries      Current state
-----+-----+-----+-----+-----+-----
    10         limit      Disable      100           0                 Within Limit
```