



# Configuration of MAC Limiting on the Cisco ASR 903 Router

---

This document describes how to configure MAC limiting on the Cisco ASR 903 Router.

- [Restrictions and Usage Guidelines, page 1](#)
- [Configuring MAC Limiting, page 1](#)

## Restrictions and Usage Guidelines

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.

## Configuring MAC Limiting

Mac address limiting per bridge-domain restricts the number of MAC addresses that the router learns in bridge-domain on an EFP, pseudowire or switchport.



### Note

Local connect feature is not supported on the Cisco ASR 903 router. However, to simulate a local connect scenario, configure the connecting EFPs on the same bridge domain and disable the mac-learning on the bridge domain by setting the MAC limit to 0. Use the **mac-address-table limit bdomain num maximum 0 action limit** command to disable mac-learning on the router.

When the total number of addresses in a bridge-domain exceeds the maximum number, the router takes a violation action. You can enable the following actions:

- Warning—The router sends a syslog message and takes no further action. The router continues learning new MAC addresses and forwarding traffic.
- Limit—The router sends a syslog message and generates a trap; MAC learning is disabled on the bridge-domain until the recovery mechanism activates. Flooding of frames with new MAC addresses

continues; to disable flooding, use the flood keyword. Flooding continues once the total number of MAC entries drops below the threshold value. This option applies only when you configure the limit keyword.

**Note**

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

- Shutdown—If the number of addresses exceeds the maximum (MAX) value, the router sends a syslog message and moves the bridge-domain (bdomain) to a disabled state. To restore the bridge-domain, disable and re-enable the mac-limiting feature.

**Before You Begin****SUMMARY STEPS**

1. **configure terminal**
2. **mac-address-table limit [bridge-domain id] [maximum num] [action {warning | limit | shutdown}] [flood]**
3. **end**
4. **show mac-address-table limit [bridge-domain id]**
5. **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>	Enter global configuration mode.
<b>Step 2</b>	<b>mac-address-table limit [bridge-domain id] [maximum num] [action {warning   limit   shutdown}] [flood]</b>	Sets the specific limit and any optional actions to be imposed at the bridge-domain level.  The default <b>maximum</b> value is 500.
<b>Step 3</b>	<b>end</b>	Return to privileged EXEC mode.
<b>Step 4</b>	<b>show mac-address-table limit [bridge-domain id]</b>	Displays the information about the MAC-address table.
<b>Step 5</b>	<b>copy running-config startup-config</b>	(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. The first instance of the mac-address-table limit command enables MAC limiting. The second instance of the command sets the limit and any optional actions to be imposed at the bridge-domain level.

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

```
Router#show mac-address-table limit bdomain 10
```

bdomain	action	flood	maximum	Total entries	Current state
10	limit	Disable	100	0	Within Limit

