Configuring MAC Address Tables

This chapter contains the following sections:

Information About MAC Addresses

To switch frames between LAN ports, the switch maintains an address table. When the switch receives a frame, it associates the media access control (MAC) address of the sending network device with the LAN port on which it was received.

The switch dynamically builds the address table by using the MAC source address of the frames received. When the switch receives a frame for a MAC destination address not listed in its address table, it floods the frame to all LAN ports of the same VLAN except the port that received the frame. When the destination station replies, the switch adds its relevant MAC source address and port ID to the address table. The switch then forwards subsequent frames to a single LAN port without flooding all LAN ports.

You can also enter a MAC address, which is termed a static MAC address, into the table. These static MAC entries are retained across a reboot of the switch.

In addition, you can enter a non-IP multicast address as a statically configured MAC address. A non-IP multicast address can accept more than one interface as its destination.

The address table can store a number of unicast and non-IP multicast address entries without flooding any frames. The switch uses an aging mechanism, defined by a configurable aging timer, so if an address remains inactive for a specified number of seconds, it is removed from the address table.

Guidelines for Configuring the MAC Address Tables

See the following guidelines and limitations for configuring the MAC address tables:

- Starting with Release 7.0(3)I2(1), the aging of the mac-address is not incrementing in the output of the **show mac address-table** CLI command. Therefore, the proper age of the mac-address cannot be determined.
- Starting with Release 7.0(3)I2(1), the **show mac address-table** CLI command does not display the multicast MAC entries. Use the **show mac address-table multicast** CLI command to check the Layer 2 entries.

MAC Address Movement

You can detect and limit the number of times that a MAC address moves from one port to another. This movement of MAC addresses between ports can cause loops. Until Cisco NX-OS Release 6.0(2)U3(1), when a loop was detected between two ports, MAC learning was disabled for 180 seconds. You can now configure the action of bringing down the port with the lower interface index when such a loop is detected by using the **mac address-table loop-detect port-down** command. To revert to the default action of disabling MAC learning, use the **no** form of this command.

Configuring MAC Addresses

Configuring Static MAC Addresses

You can configure static MAC addresses for the switch. These addresses can be configured in interface configuration mode or in VLAN configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **mac-address-table static** *mac_address* **vlan** *vlan-id* {**drop** | **interface** {*type slot*/*port*} | **port-channel** *number*} [**auto-learn**]	Specifies a static address to add to the MAC address table. If you enable the **auto-learn** option, the switch will update the entry if the same MAC address is seen on a different port.
Step 3	(Optional) switch(config)# **no mac address-table static** *mac_address* **vlan** *vlan-id*	Deletes the static entry from the MAC address table. Use the **mac address-table static** command to assign a static MAC address to a virtual interface.

Example

This example shows how to put a static entry in the MAC address table:

```
switch# configure terminal
switch(config) # mac address-table static 12ab.47dd.ff89 vlan 3 interface ethernet 1/4
switch(config) #
```

Configuring the Aging Time for the MAC Table

You can configure the amount of time that an entry (the packet source MAC address and port that packet ingresses) remains in the MAC table. MAC aging time can be configured in either interface configuration mode or in VLAN configuration mode.

Note If the Cisco Nexus device is used as a Layer 2 or Layer 3 termination switch, Cisco recommends that you set the **mac-address-table aging-time** to 1800 (higher than the default ARP aging time of 1500 seconds) on all VLANs.

The Cisco Nexus 3000 series switches do not support per-VLAN CAM aging timers.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **mac-address-table aging-time** *seconds*	Specifies the time before an entry ages out and is discarded from the MAC address table. **Note** Starting with Release 7.0(3)I2(1), the aging of the mac-address is not incrementing in the output of the **show mac address-table** CLI command. Therefore, the proper age of the mac-address cannot be determined. The *seconds* range is from 0 to 1000000. The default is 300 seconds for Cisco NX-OS 5500 and 1800 for Cisco NX-OS 5600 and 6000 series. Entering the value 0 disables the MAC aging.

Example

This example shows how to set the aging time for entries in the MAC address table to 300 seconds:

```
switch# configure terminal
switch(config) # mac-address-table aging-time 300
switch(config) # show mac address-table
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False
   VLAN     MAC Address      Type      age     Secure NTFY Ports
```

```
---------+-----------------+--------+---------+------+----+------------------
*    1     c08c.60a7.4667   dynamic  0         F      F    Eth1/9
*  300     c08c.60a7.4667   dynamic  0         F      F    nve1(3.3.3.3)
G    -     7cad.74c8.d747   static   -         F      F    sup-eth1(R)
switch(config)#
```

Configuring MAC Move Loop Detection

When the number of MAC address moves between two ports exceeds a threshold, it forms a loop. Until Cisco NX-OS Release 6.0(2)U3(1), when a loop was detected between two ports, MAC learning was disabled for 180 seconds. You can now configure the action of bringing down the port with the lower interface index when such a loop is detected by using the **mac address-table loop-detect port-down** command. To revert to the default action of disabling MAC learning, use the **no** form of this command.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)#[**no**] **mac address-table loop-detect port-down**	Specifies the port-down action for MAC move loop detection. The **no** form of this command reverts to the default action of disabling MAC learning for 180 seconds.
Step 3	switch(config)# **mac address-table loop-detect port-down edge-port**	Enables the err-disabled detection for the edge-port on the MAC move loop detection.

Disabling MAC Address Learning on Layer 2 Interfaces

You can now disable and re-enable MAC address learning on Layer 2 interfaces.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type slot/port*	Enters the interface configuration mode for the specified interface.
Step 3	switch(config-if)# **[no] switchport mac-learn disable**	Disables MAC address learning on Layer 2 interfaces. The **no** form of this command re-enables MAC address learning on Layer 2 interfaces.
Step 4	switch(config-if)# **clear mac address-table dynamic interface** *type slot/port*	Clears the MAC address table for the specified interface.

	Command or Action	Purpose
		Important After disabling MAC address learning on an interface, ensure that you clear the MAC address table.

Example

This example shows how to disable MAC address learning on Layer 2 interfaces:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# switchport mac-learn disable
switch(config-if)# clear mac address-table dynamic interface ethernet 1/4
```

This example shows how to re-enable MAC address learning on Layer 2 interfaces:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no switchport mac-learn disable
```

Clearing Dynamic Addresses from the MAC Table

You can clear all dynamic entries in the MAC address table.

Command	Purpose
switch(config)# **clear mac-address-table dynamic** {**address** *mac-addr*} {**interface** [*type slot*/*port* | **port-channel** *number*} {**vlan** *vlan-id*}	Clears the dynamic address entries from the MAC address table.

This example shows how to clear the dynamic entries in the MAC address table:

```
switch# clear mac-address-table dynamic
```

Verifying the MAC Address Configuration

Note On Cisco Nexus 3000 and Cisco Nexus 3548 Series platforms, the self router MAC or HSRP VMAC are dynamically learned by the switch under the following condition:

- When there is a transient loop in the network due to which the switch receives its own packets.

This behavior is different from other Cisco Nexus platforms. However, there is no operational impact due to these self MAC entries that are present in the MAC table. Any packet that is destined to the router MAC or HSRP MAC is routed. There is no Layer 2 lookup on these packets.

Use one of the following commands to verify the configuration:

Table 1: MAC Address Configuration Verification Commands

Command	Purpose
show mac-address-table aging-time	Displays the MAC address aging time for all VLANs defined in the switch.
show mac-address-table	Displays the contents of the MAC address table. **Note** IGMP snooping learned MAC addresses are not displayed.
show mac address-table loop-detect	Displays the currently configured action.

This example shows how to display the MAC address table:

```
switch# show mac-address-table
VLAN      MAC Address       Type    Age       Port
---------+-----------------+-------+---------+------------------------------
1         0018.b967.3cd0    dynamic 10        Eth1/3
1         001c.b05a.5380    dynamic 200       Eth1/3
Total MAC Addresses: 2
```

This example shows how to display the current aging time:

```
switch# show mac-address-table aging-time
Vlan  Aging Time
----- ----------
1     300
13    300
42    300
```

This example shows how to display the currently configured action:

```
switch# configure terminal
switch(config)# show mac address-table loop-detect
Port Down Action Mac Loop Detect : enabled
```

```
switch# configure terminal
switch(config)# no mac address-table loop-detect port-down
switch(config)# show mac address-table loop-detect
Port Down Action Mac Loop Detect : disabled
```

Triggering the Layer 2 Consistency Checker

You can manually trigger the Layer 2 consistency checker to compare the hardware and software configuration of MAC addresses and display the results. It displays MAC addresses that are configured in the software, but not configured in the hardware, as well as MAC addresses that are configured in the hardware, but not in the software. To manually trigger the Layer 2 consistency checker and display the results, use the following command in any mode:

Procedure

	Command or Action	Purpose
Step 1	switch# **show consistency-checker l2**	Starts a Layer 2 consistency check on MAC addresses and displays the results.

Example

This example shows how to trigger a Layer 2 consistency check and display the results:

```
switch# show consistency-checker l2
Consistency Check: FAILED
Legend:         * - primary entry, G - Gateway MAC, (R) - Routed MAC        age - seconds
since last
 seen


 Missing entries in the MAC Table
   VLAN     MAC Address      Type      age     Secure NTFY   Ports
---------+-----------------+--------+---------+------+----+------------------
  1        0100.0100.0106    dynamic     -        F     F    0
  1        0200.0100.0125    static      -        F     F    0


 Extra and Discrepant entries in the MAC Table
   VLAN     MAC Address      Type      age     Secure NTFY   Ports
---------+-----------------+--------+---------+------+----+------------------
* 1        0000.0100.0109    dynamic   370        F    F  Eth1/41
```