Configuring MAC Address Tables

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.

You cannot enter a multicast address as a statically configured MAC address, both for IP multicast and non-IP multicast MAC addresses. This is not supported by the N3548 platform.

The address table can store a number of unicast 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.

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.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **mac address-table static** *mac_address* **vlan** *vlan-id* {**drop** | **interface** {*type slot*/*port*} | **port-channel** *number*}
3. (Optional) switch(config)# **no mac address-table static** *mac_address* **vlan** *vlan-id*

DETAILED STEPS

	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*}	Specifies a static address to add to the MAC address table.
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) #
```

Disabling MAC Address Learning on Layer 2 Interfaces

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **[no] switchport mac-learn disable**
4. switch(config-if)# **clear mac address-table dynamic interface** *type slot/port*

DETAILED STEPS

	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.

	Command or Action	Purpose
		The **no** form of this command re-enables MAC address learning on Layer 2 interfaces. **Note** In Warp mode, the Cisco Nexus 3500 switch does not flood Layer 3 traffic to the VLAN in which the port configured using **switchport mac-learn disable** is present, and the traffic is dropped. In Normal mode, the switch should flood the Layer 3 traffic to this VLAN.
Step 4	switch(config-if)# **clear mac address-table dynamic interface** *type slot/port*	Clears the MAC address table for the specified interface. **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
```

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) remain in the MAC table. MAC aging time can be configured in either interface configuration mode or in VLAN configuration mode.

Note The Cisco Nexus device does not support per-VLAN CAM aging timers.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **mac-address-table aging-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
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. The *seconds* range is from 0 to 1000000. The default is 1800 seconds. 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 1800 seconds (30 minutes):

```
switch# configure terminal
switch(config) # mac-address-table aging-time 1800
switch(config) #
```

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
```

Configuring MAC Move Loop Detection

When the number of MAC address moves between two ports exceeds a threshold, it forms a loop. You can 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.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **[no] mac address-table loop-detect port-down**
3. switch(config)# **mac address-table loop-detect port-down edge-port**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
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.

Example

This example shows how to configure port-down as the action for MAC move loop detection.

```
switch# configure terminal
switch(config)# mac address-table loop-detect port-down
```

This example shows how to enable the err-disabled detection for the edge-port on the MAC move loop detection.

```
switch# configure terminal
switch(config)# mac address-table loop-detect port-down edge-port
```

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 conditions:

- When there is a transient loop in the network due to which the switch receives its own packets.
- When there are spoofed packets where the source MAC is same as the Router MAC or HSRP MAC.

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
```

MAC Move Loop Detection

Cisco Nexus 3548 Series switches leverage L2FM for software MAC learning (and, subsequently, loop detection). If a host (MAC address) moves between two interfaces within the same VLAN, it would trigger a MAC move. If there are a large number of such MAC moves in a short duration of time, the control plane of the switch and the CPU performance could get impacted. L2FM protects the switch from such scenarios by disabling MAC learning on the specific VLAN once the number of MAC moves for the corresponding MAC address exceeds a threshold.

For Cisco Nexus 3548 switches, the MAC move learn disable threshold criteria is when a single MAC addresses moves 10 or more times in a duration of one second within the same VLAN. Once threshold limit is hit, all new MAC learning on the corresponding VLAN is disabled for a period between 120 seconds to 240 seconds within the same VLAN. After that, new MAC learning is re-enabled on that VLAN. There is no impact of this on rest of the VLANs on the switch.

Note If Cisco Nexus 3548 Series switches is operated in N9K mode, the generated syslog messages will be similar to Cisco Nexus 9000 Series switches.

Generating Syslog Error Messages

To see MAC move notifications in syslogs, follow the below steps:

SUMMARY STEPS

1. **config t**
2. **logging level l2fm 5**
3. (Optional) **mac address-table notification mac-move**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**config t**
	Example:
	`switch# config t`
	`switch(config)#`
		Enters configuration mode.

Step 2	**logging level l2fm 5** **Example:** `switch(config)# logging level l2fm 5`	Enables logging of all L2FM events from level 5 up to the highest severity events.
Step 3	(Optional) **mac address-table notification mac-move** **Example:** `switch(config)# mac address-table notification mac-move`	Enables MAC move notification on the switch. **Note** • MAC move notification is enabled by default. • This command ensures that the syslog for L2FM detect displays when there is a MAC address move.

Following are the sample generated syslog messages:

- When MAC move is detected:

```
2018 Nov 14 16:04:23.881 N9K %L2FM-4-L2FM_MAC_MOVE2: Mac XXXX.XXXX.XXXX
in vlan 741 has moved between Po6 to Eth1/3
```

- When MAC learning on VLAN is disabled:

```
2016 Apr 11 18:00:18 %L2FM-2-L2FM_MAC_FLAP_DISABLE_LEARN_N3K: Loops detected in the
network for mac XXXX.XXXX.XXXX among ports Eth1/48 and Eth1/50/3 on vlan 4 - Disabling
 dynamic learning notifications for a period between 120 and 240 second
```

- When MAC learning on VLAN is re-enabled:

```
2023 Nov 29 21:23:19 N-3164Q-40G %L2FM-2-L2FM_MAC_FLAP_RE_ENABLE_LEARN:
Re-enabling learning in vlan 500
```

Example

In order to check if the MAC addresses move, enter the command:

```
switch# show mac address-table notification mac-move
MAC Move Notify Triggers: 1206
Number of MAC Addresses added: 944088
Number of MAC Addresses moved: 265
Number of MAC Addresses removed: 943920
```

Note The following are the possible causes for MAC moves:

- MAC addresses move because of server NIC teaming and moving between Active-Active, Active-Standby states, etc.
- MAC addresses move because the source of the data is physically moved across all switches while STP states are converged and in correct states.
- Due to loops in the network.