

Catalyst 6500/6000 Switches ARP or CAM Table Issues Troubleshooting

Document ID: 71079

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Troubleshoot ARP or CAM Related Issues

- Loss of Dynamic MAC Addresses with Distributed Switching
- CEF Drops Packets at Regular Intervals
- Switch Filter All-Zero MAC Addresses from the CAM Table
- Unicast Flooding in the Network Every 5 Minutes
- ARP Issues in Hybrid CatOS
- Error EARL-2-EARL4LOOKUPRAMERROR During the CAM Table Lookup
- Static CAM Entries Lost After Supervisor Switchover
- %ACL-5-TCAMFULL: acl engine TCAM table is full
- Ping Issues Occur when the MSFC Does Not Respond to the ARP Request in Catalyst 6500 Series

Switches

- Multiple Entries in MAC Address Table
- Virtual IP Address Used by Microsoft Load Balancing is Not Reachable

Related Information

Introduction

This document provides information on how to troubleshoot Address Resolution Protocol (ARP) or Content Addressable Memory (CAM) table-related issues on Catalyst 6500/6000 Switches.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Catalyst switches maintain several types of tables that are tailored for Layer 2 switching or multilayer switching (MLS), and are kept in very fast memory so that many fields within a frame or packet can be compared in parallel.

- **ARP** Maps an IP address to a MAC address in order to provide IP communication within a Layer 2 broadcast domain. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and only Host A responds with its MAC address.
- **CAM** All Catalyst switch models use a CAM table for Layer 2 switching. As frames arrive on switch ports, the source MAC addresses are learned and recorded in the CAM table. The port of arrival and the VLAN are both recorded in the table, along with a timestamp. If a MAC address learned on one switch port has moved to a different port, the MAC address and timestamp are recorded for the most recent arrival port. Then, the previous entry is deleted. If a MAC address is found already present in the table for the correct arrival port, only its timestamp is updated.
- **Ternary Content Addressable Memory (TCAM)** In multilayer switches, all the processes that access control lists (ACLs) provide in traditional routing, such as matching, filtering, or control specific traffic, are implemented in hardware. TCAM allows a packet to be evaluated against an entire access list in a single table lookup. Most switches have multiple TCAMs so that both inbound and outbound security, as well as QoS ACLs, can be evaluated simultaneously, or entirely in parallel with a Layer 2 or Layer 3 forwarding decision.

Troubleshoot ARP or CAM Related Issues

Loss of Dynamic MAC Addresses with Distributed Switching

In distributed switching, each Distributed Feature Card (DFC) is responsible for maintaining each own CAM table. This means that each DFC learns the MAC address and ages them, which depends on the CAM aging and traffic matching that particular entry. With distributed switching, it is normal that the supervisor engine does not see any traffic for a particular MAC address for a while, so the entry might expire. There are currently two mechanisms available to keep the CAM tables consistent between the different engines, such as DFC (present in line modules) and Policy Feature Card (PFC) (present in supervisor modules):

- Flood to Fabric (FF)
- MAC Notification (MN)

When a MAC address entry is aged out on the PFC, the **show mac-address address <MAC_Address> all** command displays the DFC or PFC that holds this MAC address.

In order to prevent the age out of an entry on a DFC or PFC, even if there is not traffic for that MAC address, enable the MAC address synchronization. Issue these commands in order to enable the synchronization:

```
!--- This is a global configuration command and is used to enable the synchronization.
```

```
Cat6K-IOS(config)#mac-address-table synchronize
```

```
!--- This is a privileged EXEC command and is used to clear dynamic MAC addresses.
```

```
Cat6K-IOS#clear mac-address-table dynamic
```

The **mac-address-table synchronize** command is available from Cisco IOS® Software Releases 12.2(18)SXE4 and later. After you enable it, it is possible to still see entries that are not present in PFC or DFC. However, the module has a way to learn it from others that use Ethernet Out of Band Channel (EOBC).



Caution: The **mac-address-table synchronize** command purges the routed MAC entries. In order to avoid this, disable the routed MAC purging with the **mac-address-table aging-time 0 routed-mac** global configuration command.

CEF Drops Packets at Regular Intervals

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology that provides superior performance compared to other switching technologies, especially in networks with dynamic traffic patterns. CEF maintains data structures called Forwarding Information Base (FIB) and adjacency tables. The FIB table mirrors the information in the routing table and is used to make forwarding decisions. The adjacency table contains the precomputed link-layer header for next hop devices. Based on the next hop interface, entries in the FIB table are mapped to entries in the adjacency table. A device is not able to perform CEF switch packets if the adjacency table is not populated with the required information.

If CEF drops packets at regular intervals, interspaced by periods of normal operation, it is probably due to the adjacency table being cleared periodically. This is caused by the aging of the ARP entry. Packets are not CEF switched for the duration in which the adjacency table is repopulated with the required next hop information. While ARP entries are refreshed by default every four hours, configuring a very small value of ARP timeout is disruptive to CEF operation.

Issue the **arp timeout** command in the interface configuration mode in order to change the time in which an entry remains in the ARP cache.

Refer to Cisco bug ID CSCeb53542 (registered customers only) for more information on this vulnerability. Refer to Troubleshooting Incomplete Adjacencies with CEF for more information on CEF adjacency.

Switch Filter All-Zero MAC Addresses from the CAM Table

The switch filter frames with a source MAC address of 00-00-00-00-00-00, which is an invalid source MAC, from the CAM table. This is an example of the syslog error output when this occurs:

```
%SYS-4-P2_WARN: 1/Filtering MAC address 00-00-00-00-00-00 on port 2/48 from host table
```

These messages are informational and tell you that a frame that has a source MAC address of 00-00-00-00-00-00 is found, and the switch will never add that to the CAM table. However, the switch will forward traffic sourced from an all-zero MAC address.

The workaround is to identify the end station that generates frames with an all-zero source MAC address. Typically, one of these devices transmits such frames:

- A traffic generator, such as Spirent SmartBits
- Certain types of servers, such as load-balancing IBM WebSphere servers
- A misconfigured router or end station, such as a device that transmits all-zeros broadcasts
- A faulty NIC

Unicast Flooding in the Network Every 5 Minutes

LAN switches use forwarding tables, such as Layer 2 and CAM tables, to direct traffic to specific ports based on the VLAN number and the destination MAC address of the frame. When there is no entry that corresponds

to the destination MAC address of the frame in the incoming VLAN, the (unicast) frame is sent to all forwarding ports within the respective VLAN. This causes flooding. The very cause of flooding is that the destination MAC address of the packet is not in the Layer 2 forwarding table of the switch. In this case, the packet is flooded out of all forwarding ports in its VLAN, except the port it is received on.

The default ARP table aging time is 4 hours while the CAM holds the entries for only 5 minutes. The switch sends out a frame to all forwarding ports within the respective VLAN when the destination MAC address is aged out from the CAM table. You need a CAM aging timer greater or equal to the ARP timeout in order to prevent unicast flooding. As a workaround, you can issue one of these commands in order to increase the CAM aging timer for the VLAN you are having trouble with to match the ARP aging time:

- For CatOS, issue the **set cam agingtime** command.
- For Cisco IOS software, issue the **mac-address-table aging-time** command.

Note: In any Catalyst environment that runs a Hot Standby Router Protocol (HSRP), it is recommended that you ensure the CAM and ARP timers are synchronized.

Refer to Unicast Flooding in Switched Campus Networks for information on possible causes and implications of unicast packet flooding in switched networks.

ARP Issues in Hybrid CatOS

In Hybrid mode, the supervisor engine runs CatOS and the Multilayer Switch Feature Card (MSFC) runs Cisco IOS. CatOS operates at Layer 2 and builds the CAM address table to hold the VLAN, MAC address and port number information. Cisco IOS in MSFC operates in Layer 3 and builds the ARP table to hold the IP address to MAC address resolution. When you change the IP address of any device, such as a printer or a server, you might not be able to ping that new IP address. However, you are able to ping the new IP address from the same VLAN. This can be an ARP issue on the MSFC.

This workaround can help to isolate and resolve the issue:

1. Clear the ARP table on the MSFC.

```
MSFC2#clear arp int vlan 40
```

2. Verify the ARP timeout value. The default value is 4 hours. If the ARP timeout in the VLAN is high, you can set the timeout value back to the default or optimal value.

```
MSFC2#show int vlan 40
Vlan40 is up, line protocol is up
  Hardware is Cat6k RP Virtual Ethernet, address is 00d0.0050.33fc (bia 00d0.0050.33fc)
  Internet address is 40.40.40.3/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:01:44, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
MSFC2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MSFC2(config)#int vlan 40
MSFC2(config-if)#arp timeout ?
<0-2147483> Seconds
```

```
MSFC2(config-if)#arp timeout 240
```

3. Reload the MSFC.

```
MSFC2#write memory
Building configuration...
[OK]
MSFC2#reload
Proceed with reload? [confirm]
Supervisor> (enable)
```

Error EARL-2-EARL4LOOKUPRAMERROR During the CAM Table Lookup

This is an example of the syslog error output when you have this issue:

```
%EARL-2-EARL4LOOKUPRAMERROR:Address eac6, data 0-0-8000-0, count 8
```

This appears when you perform a CAM table lookup. This occurs due to a parity error when you access memory. This error is usually generated when you issue the **show cam** command in order to access the CAM table. In some cases, the switch also resets when the **show cam** command is issued.

```
%EARL-2-EARL4LOOKUPRAMERROR: Address [hex], data [hex]-[hex]-[hex]-[hex], count [dec]
```

This error message indicates that a lookup RAM parity error has been detected. The address [hex] field is the address in the forwarding table where the error was detected. The data [hex]-[hex]-[hex]-[hex] field is the word0, word1, word2, and word3 of RAM data that generated the parity error. The count [dec] field is the total number of parity errors.

This message is not catastrophic and might not result in outage situations if you only have isolated occurrences of it. If you receive this message continuously, it indicates that the switch is trying to write to a bad DRAM sector when it adds a new entry to the CAM table. Then, you need to replace the DRAM or the supervisor itself.

Static CAM Entries Lost After Supervisor Switchover

Static CAM entries that are configured on the active supervisor engine are lost after fast switchover. As a workaround to this issue, you must reconfigure CAM entries after fast switchover.

Refer to Cisco bug IDs CSCed87627 (registered customers only) and CSCee27955 (registered customers only) for more information on this vulnerability.

%ACL-5-TCAMFULL: acl engine TCAM table is full

If the TCAM is full and you attempt to add new ACLs, or access control entries (ACEs) to ACLs that exist, the commit or map process fails. Any prior configuration remains in effect. In the case of Router Access Control Lists (RACLs), the ACL is enforced in software on the Multilayer Switch Feature Card (MSFC) with the corresponding performance penalty.

On a switch that runs hybrid software, if you configure a Virtual Local Area Network Access Control List (VACL) or QoS ACL ACEs that exceed the pattern or mask capacity of the TCAM, a syslog message similar to this prints to the console:

```
%ACL-5-TCAMFULL: acl engine TCAM table is full
```

On Supervisor IOS systems, or on the MSFC in a hybrid system, if you configure RACL ACEs that exceed the capacity of the TCAM, a syslog message similar to this prints to the console:

```
%FM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

On Supervisor IOS systems, or on the MSFC in a hybrid system, issue the **show fm summary** command in order to see which interfaces enforce ACLs in hardware (ACTIVE) and which interfaces enforce ACLs in software (INACTIVE).

The workaround for this issue is to remove the unused ACL or QoS from the switch configuration. Refer to Understanding ACL on Catalyst 6500 Series Switches for more information.

Ping Issues Occur when the MSFC Does Not Respond to the ARP Request in Catalyst 6500 Series Switches

When you ping a VLAN interface, an ARP request with a source IP of that VLAN is sent to the Default Router (MSFC), but the router does not respond to the ARP request and the debug ARP shows this error message:

```
IP ARP req filtered src [ip-address] [mac-address] dst [ip-address]
[mac-address] wrong cable, interface-id
```

For each ARP datagram, an ARP reply is discarded if the destination IP address does not match the local host address. An ARP request is discarded if the source IP address is not in the same subnet. It is desirable that this test be overridden by a configuration parameter in order to support the infrequent cases where more than one subnet can co-exist on the same cable.

An ARP reply is generated only if the destination protocol IP address is reachable from the local host, as determined by the routing algorithm, and the next hop is not through the same interface. If the local host functions as a gateway, this can result in ARP replies for destinations not in the same subnet. This shows that to drop the ARP request is justifiable.

This can be resolved by making the Catalyst 6500 not respond to all ARP requests because the source IP address in the ARP request is on a different subnet than the target IP address in the ARP. Therefore, the MSFC/Router concludes that the ARP did not remain in the same Layer 2 domain and shows the wrong cable type. In other words, the wrong cable debug message is generated when the ARP source and destination do not belong to the same Layer 2 domain. In order to make ARP work in this scenario, the destination protocol IP must be reachable with the use of the static route as a workaround.

Multiple Entries in MAC Address Table

Two entries show for MAC address in the MAC address table.

```
Cat6K#show mac-address-table int gi 6/11
Displaying entries from Line card 6:
```

```
Legend: * - primary entry
         age - seconds since last seen
         n/a - not available
```

vlan	mac address	type	learn	age	ports
[FE 1]:					
* 100	0011.857c.4d10	dynamic	Yes	0	Gi6/11
[FE 2]:					
* 100	0011.857c.4d10	dynamic	Yes	95	Gi6/11

```
Cat6K#show module 6
Mod Ports Card Type
```

```
Model
```

```
Serial No.
```

```

-----
 6   48  CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SADxxxxxxxx
Mod MAC addresses                               Hw   Fw           Sw           Status
-----
 6  001d.45fd.xx4a to 001d.45fd.xx79   2.6  12.2(14r)S5  12.2(18)SXF8 Ok
Mod Sub-Module                               Model          Serial          Hw           Status
-----
 6  Distributed Forwarding Card WS-F6700-DFC3B   SALxxxxxxxxx  4.6           Ok

Mod Online Diag Status
-----
 6  Pass

```

Two Layer 2 forwarding lookup engines exist in the DFC environment. It is common in the dCEF environment that the FE1 and FE2 learn the same MAC address on the same port on a CEF720/dCEF720 architecture line cards.

Virtual IP Address Used by Microsoft Load Balancing is Not Reachable

Cisco routers require an ARP (Address Resolution Protocol) entry for every virtual IP address. While network load balancing uses Level 2 multicast for the delivery of packets. In Cisco's implementation of the RFC, multicast is used only for IP multicast. Therefore, when the router does not see a multicast IP address, it does not automatically create an ARP entry, and you must manually add it to the router.

Normally, Cisco devices do not put a multicast MAC address (clusters virtual MAC address) in the ARP table if it was resolved through a unicast IP address (cluster's virtual address). In order to resolve this issue, you need a static mapping of the unicast virtual IP address to the multicast MAC address.

For more information, refer to the Multicast Mode section of the *Catalyst Switches for Microsoft Network Load Balancing Configuration Example*.

Related Information

- [Troubleshooting Incomplete Adjacencies with CEF](#)
 - [Unicast Flooding in Switched Campus Networks](#)
 - [LAN Product Support](#)
 - [LAN Switching Technology Support](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 27, 2009

Document ID: 71079
