Understand ASA High Availability MAC Table Synchronization on Transparent Mode with HSRP Routers

Contents

Introduction

This document describes the behavior of a pair of ASA connected to a cluster of routers that use HSRP.

Prerequisites

- Adaptive Security Appliance (ASA)
- ASA High Availability (HA).
- Hot Standby Router Protocol (HSRP).
- Firewall in transparent mode.

Components Used

- 2 CSR routers with HSRP.
- 2 ASA configured in HA which points to the HSRP pair.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

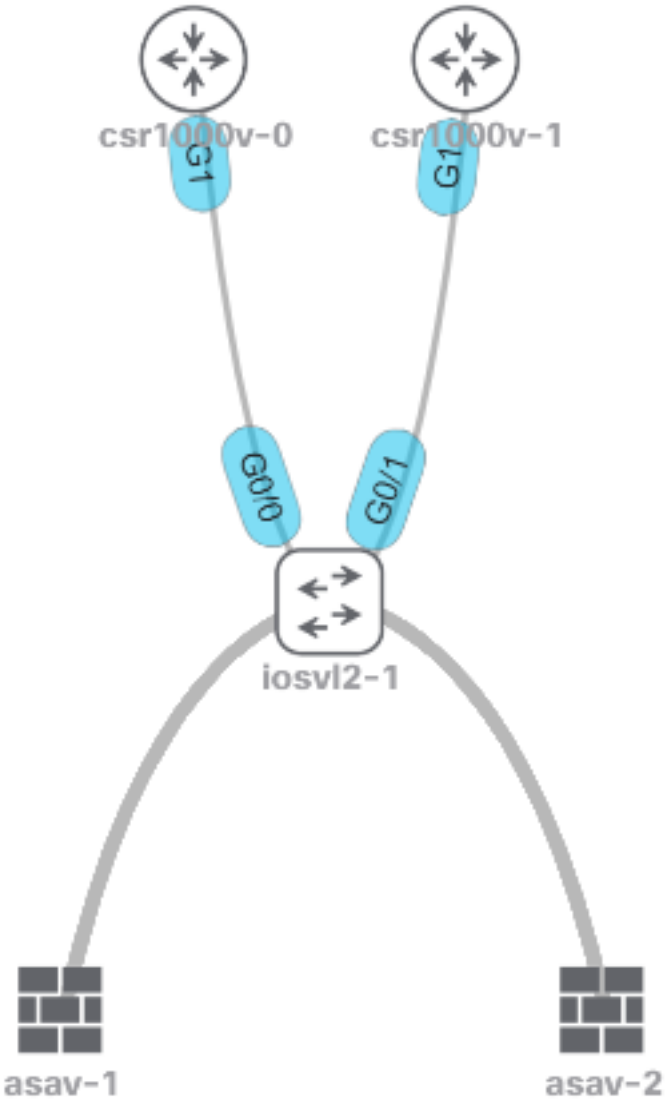
Background Information

For a pair of ASA configured in High Availability transparent mode, if the pair of firewalls are upstream connected to a cluster of routers and those adjacent routers use HSRP, the traffic from the firewalls destines to the router IP address which also points to the MAC Address of a specific router. However, if the return traffic is sourced from the MAC address of another router interface in

the HSRP pair, it can cause a network outage.

The problem is that the mac-address-table age timeout is 5 min (300 seconds), and the Address Resolution Protocol (ARP) timeout is 14400 seconds by default. Because the next-hop router uses HSRP, there is never any traffic sourced from the HSRP MAC address. If this happens, the mac-address-table entry on the ASA expires and traffic fails.

Network Diagram



Troubleshoot

Understand MAC table synchronization for ASA HA in transparent mode with HSRP

These outputs show how ASA units synchronize their MAC table when the active unit learns new and deletes old entries.

Active unit **asav-1** loses **5254.0017.8a8c** MAC address from one of the HSRP routers, in this case, **csr1000v-0**.

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
inside 5254.001f.dfa8 dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

You can see how **5254.0017.8a8c** disappears after 5 minutes.

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

The standby unit does not lose the **5254.0017.8a8c** MAC entry. This behavior can cause confusion, however, it is totally expected.

The standby unit does not update the MAC address table unless it becomes the new active unit.

The Standby unit keeps **5254.0017.8a8c** after several hours and stays at one (1) minute of age time all the time.

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

You can wait hours/days and run the same command and see the same result.

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

Furthermore, if you issue the **show failover** command, there are no changes on **L2BRIDGE Tbl** counter when the Active unit loses the HSRP entry.

```
Stateful Failover Logical Update Statistics
Link : failoverlink GigabitEthernet0/3 (up)
Stateful Obj xmit xerr rcv rerr
General 86751 0 77968 8
sys cmd 77854 0 77853 0
up time 0 0 0 0
```

```
RPC services 0 0 0 0
<--- More --->

TCP conn 0 0 0 0
UDP conn 8882 0 90 0
ARP tbl 4 0 1 0
L2BRIDGE Tbl 3 0 22 0
Xlate_Timeout 0 0 0 0
IPv6 ND tbl 0 0 0 0
SIP Session 0 0 0 0
SIP Tx 0 0 0 0
SIP Pinhole 0 0 0 0
Route Session 8 0 0 8
```

MAC Address Table Entry Ages out due to Asymmetric Routing

When traffic flows directly between two MAC addresses through the transparent firewall, those addresses do not age out while traffic flows because the ASA receives frames sourced from the two MAC addresses which send the traffic.

When traffic flow is asymmetric the entry times out if the ASA does not receive a response from that specific MAC address.

> **Note**: Asymmetric routing means the ASA sees traffic destined to a specific MAC address, but not traffic sourced from that same MAC address

The symptoms of this problem are that after the ASA ages out the MAC address entry (after 5 minutes of no traffic sourced from that MAC address), traffic destined to that MAC address is dropped until the MAC entry is populated again.

Usually, the problem presents itself when it shows that connectivity to a server is re-established after one or two tries, and this is because the first packet is dropped so that the ASA can go through the steps to learn the location of a MAC address.

Suggested solution

In order to solve this problem, add a static MAC address entry table for the HSRP IP on the Firewall, or increase the age time to some value such that an ARP reply comes from the corresponding HSRP router before the entry times out.

The better solution is to add a static MAC entry since it is unsure if the ASA receives an ARP reply from HSRP active router.

Related Information

- **Technical Support & Documentation - Cisco Systems**