

# Entender la sincronización de la tabla MAC de alta disponibilidad ASA en modo transparente con routers HSRP

## Contenido

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Troubleshoot](#)

[Comprender la sincronización de la tabla MAC para ASA HA en modo transparente con HSRP](#)

[La entrada de la tabla de direcciones MAC caduca debido al enrutamiento asimétrico](#)

[Solución sugerida](#)

[Información Relacionada](#)

## Introducción

Este documento describe el comportamiento de un par de ASA conectados a un clúster de routers que utilizan HSRP.

## Prerequisites

- Dispositivo de seguridad adaptable (ASA)
- ASA High Availability (HA).
- Protocolo de rHot Standby Router Protocol (HSRP).
- Firewall en modo transparente.

## Componentes Utilizados

- 2 routers CSR con HSRP.
- 2 ASA configurado en HA que apunta al par HSRP.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

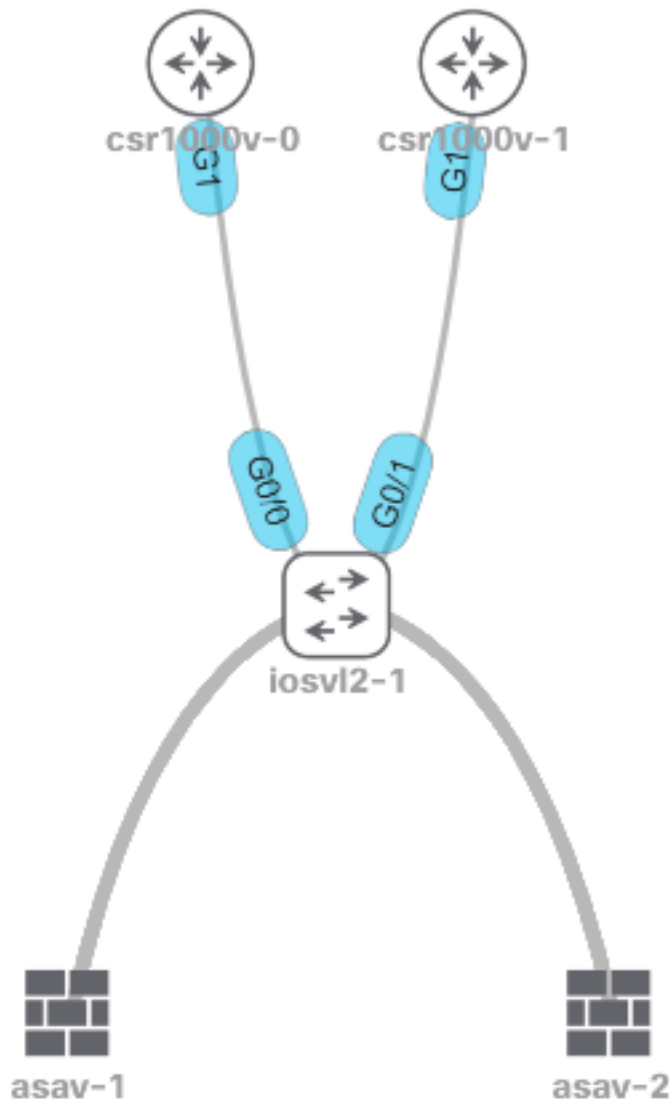
## Antecedentes

Para un par de ASA configurados en modo transparente de alta disponibilidad, si el par de firewalls están conectados en sentido ascendente a un clúster de routers y esos routers adyacentes utilizan HSRP, el tráfico de los firewalls se dirige a la dirección IP del router, que también señala a la dirección MAC de un router específico. Sin embargo, si el tráfico de retorno

se origina en la dirección MAC de otra interfaz de router en el par HSRP, puede causar una interrupción en la red.

El problema es que el tiempo de espera de la tabla de direcciones mac es de 5 minutos (300 segundos) y el tiempo de espera del Protocolo de resolución de direcciones (ARP) es de 14400 segundos de forma predeterminada. Dado que el router de salto siguiente utiliza HSRP, nunca hay tráfico originado en la dirección MAC de HSRP. Si esto sucede, la entrada mac-address-table en ASA expira y el tráfico falla.

## Diagrama de la red



## Troubleshoot

Comprender la sincronización de la tabla MAC para ASA HA en modo transparente con HSRP

Estos resultados muestran cómo las unidades ASA sincronizan su tabla MAC cuando la unidad activa aprende nuevas entradas y elimina entradas antiguas.

La unidad activa **asav-1** pierde la dirección MAC **5254.0017.8a8c** de uno de los routers HSRP, en este caso, **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
```

Puede ver cómo **5254.0017.8a8c** desaparece después de 5 minutos.

```
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
```

La unidad standby no pierde la entrada MAC **5254.0017.8a8c**. Este comportamiento puede causar confusión, sin embargo, es totalmente esperado.

La unidad standby no actualiza la tabla de direcciones MAC a menos que se convierta en la nueva unidad activa.

La unidad en espera mantiene **5254.0017.8a8c** después de varias horas y permanece en un (1) minuto de edad todo el tiempo.

```
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
```

Puede esperar horas/días y ejecutar el mismo comando y ver el mismo resultado.

```
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
```

Además, si emite el **show failover** , no hay cambios en el contador **L2BRIDGE Tbl** cuando la unidad activa pierde la entrada HSRP.

```
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
```

## La entrada de la tabla de direcciones MAC caduca debido al enrutamiento asimétrico

Cuando el tráfico fluye directamente entre dos direcciones MAC a través del firewall transparente, esas direcciones no caducan mientras el tráfico fluye porque ASA recibe tramas originadas en las dos direcciones MAC que envían el tráfico.

Cuando el flujo de tráfico es asimétrico, la entrada se agota si ASA no recibe una respuesta de esa dirección MAC específica.

**Nota:** El ruteo asimétrico significa que ASA ve el tráfico destinado a una dirección MAC específica, pero no el tráfico originado en esa misma dirección MAC

Los síntomas de este problema son que después de que el ASA desactualiza la entrada de la dirección MAC (después de 5 minutos de que no haya tráfico originado en esa dirección MAC), el tráfico destinado a esa dirección MAC se descarta hasta que la entrada MAC se rellena nuevamente.

Por lo general, el problema se presenta cuando muestra que la conectividad a un servidor se restablece después de uno o dos intentos, y esto se debe a que el primer paquete se descarta para que el ASA pueda seguir los pasos para aprender la ubicación de una dirección MAC.

## Solución sugerida

Para resolver este problema, agregue una tabla de entrada de dirección MAC estática para la IP HSRP en el firewall, o aumente el tiempo de antigüedad a algún valor tal que una respuesta ARP provenga del router HSRP correspondiente antes de que se agote el tiempo de espera de entrada.

La mejor solución es agregar una entrada MAC estática ya que no está seguro si ASA recibe una respuesta ARP del router HSRP activo.

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).