了解使用HSRP路由器的透明模式上的ASA高可用性MAC表同步

目录

简介

本文档介绍连接到使用HSRP的路由器集群的一对ASA的行为。

先决条件

- 自适应安全设备(ASA)
- ASA高可用性(HA)。
- 热备份路由器协议(HSRP)。
- 透明模式下的防火墙。

使用的组件

- 2台具有HSRP的CSR路由器。
- 2在HA中配置的ASA指向HSRP对。

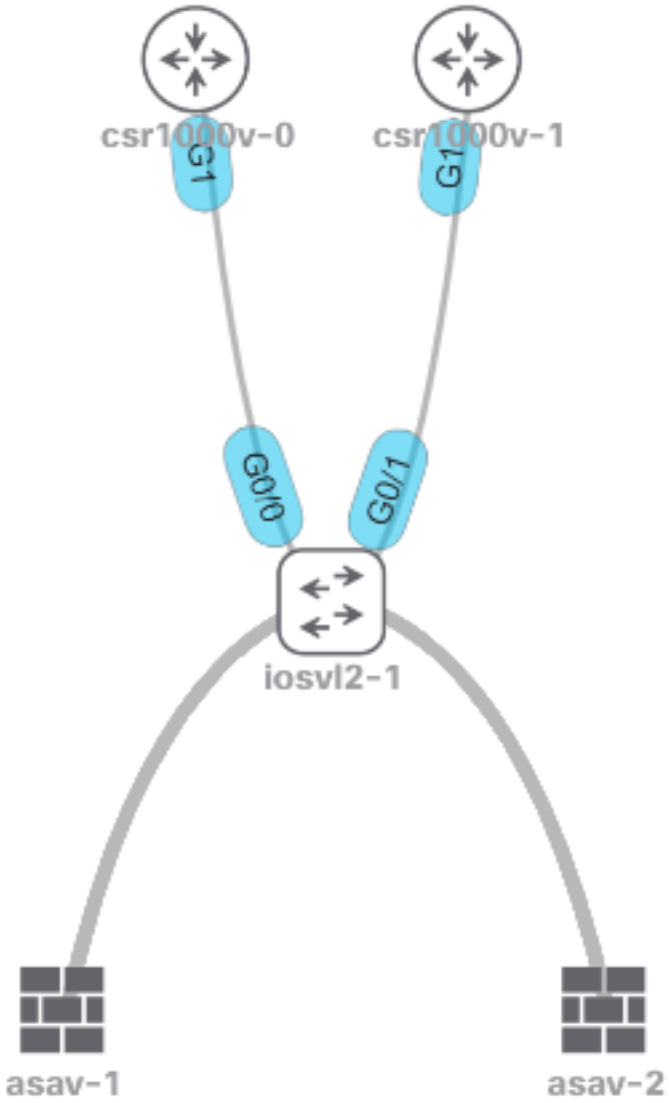
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

对于在高可用性透明模式下配置的一对ASA，如果一对防火墙上游连接到路由器集群，并且这些相邻路由器使用HSRP，则来自防火墙的流量将指向路由器IP地址，该地址也指向特定路由器的MAC地址。但是，如果返回流量源自HSRP对中另一个路由器接口的MAC地址，则可能导致网络中断。

问题是mac-address-table age timeout为5分钟（300秒），默认情况下地址解析协议(ARP)超时为14400秒。由于下一跳路由器使用HSRP，因此从没有来自HSRP MAC地址的任何流量。如果发生这种情况，则ASA上的mac-address-table条目会过期，并且流量会失败。

网络图



故障排除

了解使用HSRP的透明模式下ASA HA的MAC表同步

这些输出显示当主用设备获取新条目并删除旧条目时ASA设备如何同步其MAC表。

主用设备**asav-1**会从其中一个HSRP路由器(在本例中为**csr1000v-0**)丢失**5254.0017.8a8c** MAC地址。

```
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
```

您可以看到**5254.0017.8a8c**在5分钟后如何消失。

```
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
```

备用设备不会丢失**5254.0017.8a8c** MAC条目。这种行为可能会引起混淆，但这是完全预料到的。

备用设备不会更新MAC地址表，除非它成为新的主用设备。

备用设备在数小时后保持**5254.0017.8a8c**，并且一直保持一(1)分钟的老化时间。

```
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
```

您可以等待数小时/数天，运行相同的命令并查看相同的结果。

```
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
```

此外，如果您发出 **show failover** 命令，当主用设备丢失HSRP条目时，**L2BRIDGE Tbl**计数器上没有更改。

```
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
```

由于非对称路由，MAC地址表条目过期

当流量直接在两个MAC地址之间通过透明防火墙传输时，这些地址不会在流量传输时老化，因为ASA接收来自发送流量的两个MAC地址的帧。

当流量不对称时，如果ASA未收到来自该特定MAC地址的响应，则条目超时。

> **注意：**非对称路由意味着ASA会看到发往特定MAC地址的流量，但不会看到源自相同MAC地址的流量

此问题的症状是，在ASA使MAC地址条目老化后（5分钟后没有源自该MAC地址的流量），流向该MAC地址的流量将被丢弃，直到再次填充MAC条目。

通常，当问题显示经过一两次尝试后重新建立与服务器的连接时，问题就会出现，这是因为第一个数据包被丢弃，因此ASA可以通过这些步骤来了解MAC地址的位置。

建议的解决方案

为了解决此问题，请在防火墙上为HSRP IP添加静态MAC地址条目表，或将老化时间增加到某个值，以使ARP应答在条目超时之前来自相应的HSRP路由器。

更好的解决方案是添加一个静态MAC条目，因为它无法确定ASA是否收到来自HSRP活动路由器的ARP应答。

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。