S5810交换机IP Source Guard典型配置

攻击检测及防范 端口安全 MAC地址认证 孔天娇 2014-04-28 发表

S5810产品IP Source Guard功能的配置

一、组网需求：

Switch A通过端口GigabitEthernet1/0/1，GigabitEthernet1/0/2，GigabitEthernet1/0/3和GigabitEthernet1/0/4分别与客户端Host A，Host B，Host C和DHCP Server相连。

具体应用需求如下：

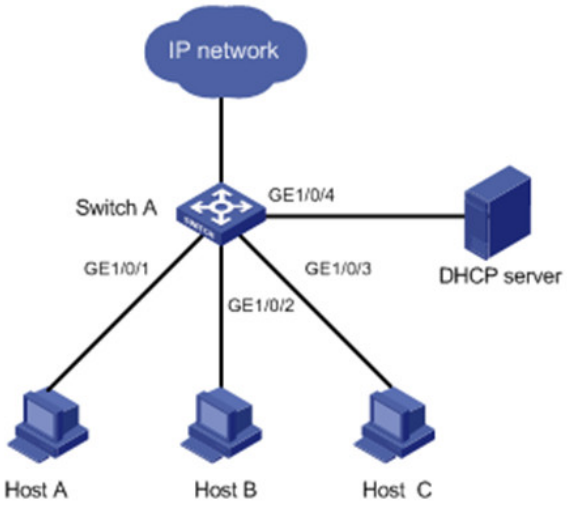
Host A的MAC地址为00-01-02-03-04-05，IP地址通过手工配置，为192.168.0.1/24。

Host B，Host C通过DHCP Server动态获取IP地址。

Switch A上开启DHCP Snooping功能，记录客户端的DHCP Snooping表项。

Switch A的端口GigabitEthernet1/0/1上配置静态绑定表项，只允许Host A发送的报文通过，在端口GigabitEthernet1/0/2，端口GigabitEthernet1/0/3上开启IP Source Guard动态绑定功能，防止客户端使用伪造的不同源IP地址对服务器进行攻击。

二、组网图：



三、配置步骤：

配置在Switch A的GigabitEthernet1/0/1上只允许MAC地址为00-01-02-03-04-05，IP地址为192.168.0.3的Host A发送的IP报文通过。

system-view
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0203-0405
[SwitchA-GigabitEthernet1/0/1] quit

设置与DHCP服务器相连的端口GigabitEthernet1/0/2为信任端口。

[SwitchA] interface GigabitEthernet1/0/4
[SwitchA-GigabitEthernet1/0/4] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/4] quit

开启DHCP Snooping功能。

[SwitchA] dhcp-snooping

配置端口GigabitEthernet1/0/2的动态绑定功能。

system-view
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] ip check source ip-address mac-address
[SwitchA-GigabitEthernet1/0/2] quit

配置端口GigabitEthernet1/0/3的动态绑定功能。

system-view
[SwitchA] interface GigabitEthernet1/0/3
[SwitchA-GigabitEthernet1/0/3] ip check source ip-address mac-address
[SwitchA-GigabitEthernet1/0/3] quit

验证配置结果

显示IP Source Guard获取的动态表项。

```
display ip check source
The following user address bindings have been configured:
     MAC          IP   Vlan       Port           Status
0001-0203-0406 192.168.0.2  1  GigabitEthernet1/0/2  DHCP-SNP   0001-0203-0407 19
2.168.0.3  1  GigabitEthernet1/0/3  DHCP-SNP
 ------------2 binding entries queried, 2 listed------------------
```

显示DHCP Snooping表项，查看其是否和IP Source Guard获取的动态表项一致。

```
display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Type IP Address     MAC Address    Lease   VLAN Interface
==== =============== ============== ============ ==== =
D  192.168.0.2   0001-0203-0406 86335   1   GigabitEthernet1/0/2
D  192.168.0.3   0001-0203-0407 86335   1   GigabitEthernet1/0/3
```

从以上显示信息可以看出，端口GigabitEthernet1/0/2，GigabitEthernet1/0/3在配置IP Source Guard动态绑定功能之后获取了DHCP Snooping表项。

四、 配置关键点：

无