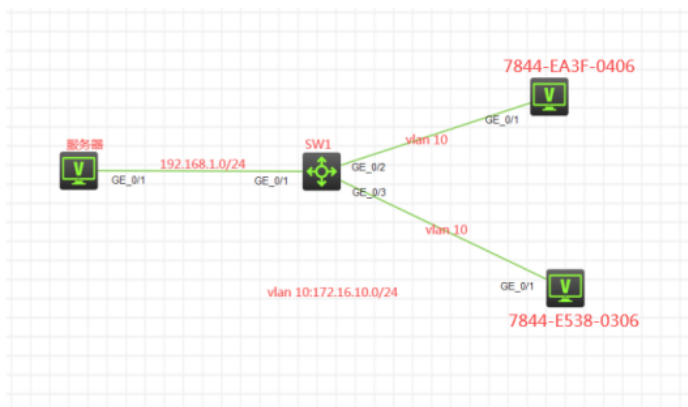


基于二层ACL典型组网配置案例

[VLAN](#)[ACL](#)[H3C模拟器](#)[韦家宁](#)

2020-02-21 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器来模拟高级ACL典型组网配置。服务器在网络拓扑图中已有明确的标识。要求使用二层ACL来限制MAC为7844-E538-0306不能访问服务器。

配置步骤

- 1、按照网络拓扑图正确配置IP地址
- 2、SW1配置二层ACL

配置关键点

第一阶段调试（基础网络配置）：

SW1：

```
<H3C>sys
```

```
System View: return to User View with Ctrl+Z.
```

```
[H3C]sysname SW1
```

```
[SW1]vlan 10
```

```
[SW1-vlan10]quit
```

```
[SW1]int vlan 10
```

```
[SW1-Vlan-interface10]ip address 172.16.10.1 24
```

```
[SW1-Vlan-interface10]quit
```

```
[SW1]int range gi 1/0/2 to gi 1/0/3
```

```
[SW1-if-range]port link-type access
```

```
[SW1-if-range]port access vlan 10
```

```
[SW1-if-range]quit
```

```
[SW1]int gi 1/0/1
```

```
[SW1-GigabitEthernet1/0/1]ip address 192.168.1.1 24
```

```
[SW1-GigabitEthernet1/0/1]quit
```

第一阶段测试：

所有PC都填写IP地址，且都能互通：

配置PC_4

接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	172.16.10.2/24	

刷新

接口管理

☐ 禁用

☒ 启用

IPv4配置:

☐ DHCP

☒ 静态

IPv4地址:172.16.10.2

掩码地址:255.255.255.0

IPv4网关:172.16.10.1

启用

配置PC_3

接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	172.16.10.3/24	

刷新

接口管理

☐ 禁用

☒ 启用

IPv4配置:

☐ DHCP

☒ 静态

IPv4地址:172.16.10.3

掩码地址:255.255.255.0

IPv4网关:172.16.10.1

启用

配置PC_2

接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	192.168.1.2/24	

刷新

接口管理

☐ 禁用

☒ 启用

IPv4配置:

☐ DHCP

☒ 静态

IPv4地址:192.168.1.2

掩码地址:255.255.255.0

IPv4网关:192.168.1.1

启用

```
hcl_h6irtl
SS820V2-54Q5-GE_1 PC_4 PC_3 PC_2
<H3C>Feb 21 13:39:08:655 2020 H3C SHELL/S/SHELL_LOGIN: Console logged in from con0.

<H3C>ping 172.16.10.3
Ping 172.16.10.3 (172.16.10.3): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.10.3: icmp_seq=0 ttl=255 time=3.000 ms
56 bytes from 172.16.10.3: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 172.16.10.3: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 172.16.10.3: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 172.16.10.3: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for 172.16.10.3 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.000/3.000/0.632 ms
<H3C>Feb 21 13:39:20:914 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 172.16.10.3
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/2.000/3.000/0.632 ms.

<H3C>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=254 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=254 time=1.000 ms
```

```
hcl_h6irtl
SS820V2-54Q5-GE_1 PC_4 PC_3 PC_2
<H3C>Feb 21 13:39:15:195 2020 H3C SHELL/S/SHELL_LOGIN: Console logged in from con0.

<H3C>ping 172.16.10.2
Ping 172.16.10.2 (172.16.10.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.10.2: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 172.16.10.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 172.16.10.2: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 172.16.10.2: icmp_seq=3 ttl=255 time=2.000 ms
56 bytes from 172.16.10.2: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 172.16.10.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.400/2.000/0.490 ms
<H3C>Feb 21 13:39:48:343 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 172.16.10.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/1.400/2.000/0.490 ms.

<H3C>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=254 time=1.000 ms
```

```
hcl_h6irtl
SS820V2-54Q5-GE_1 PC_4 PC_3 PC_2
<H3C>Feb 21 13:39:12:297 2020 H3C SHELL/S/SHELL_LOGIN: Console logged in from con0.

<H3C>ping 172.16.10.2
Ping 172.16.10.2 (172.16.10.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.10.2: icmp_seq=0 ttl=254 time=2.000 ms
56 bytes from 172.16.10.2: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 172.16.10.2: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 172.16.10.2: icmp_seq=3 ttl=254 time=1.000 ms
56 bytes from 172.16.10.2: icmp_seq=4 ttl=254 time=1.000 ms

--- Ping statistics for 172.16.10.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
<H3C>Feb 21 13:40:06:758 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 172.16.10.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/1.200/2.000/0.400 ms.

ping 172.16.10.3
Ping 172.16.10.3 (172.16.10.3): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.10.3: icmp_seq=0 ttl=254 time=2.000 ms
56 bytes from 172.16.10.3: icmp_seq=1 ttl=254 time=2.000 ms
56 bytes from 172.16.10.3: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 172.16.10.3: icmp_seq=3 ttl=254 time=2.000 ms
56 bytes from 172.16.10.3: icmp_seq=4 ttl=254 time=2.000 ms

--- Ping statistics for 172.16.10.3 ---
```

第二阶段调试（二层ACL关键配置点）：

先查看ARP表：

```
[SW1]dis arp
Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid
IP address MAC address SVLAN/VSI Interface/Link ID Aging Type
172.16.10.2 7844-ea3f-0406 10 GE1/0/2 14 D
172.16.10.3 7844-e538-0306 10 GE1/0/3 17 D
192.168.1.2 7844-c068-0206 -- GE1/0/1 15 D
[SW1]]
```

```
[SW1]acl mac 4000
[SW1-acl-mac-4000]rule 0 deny source-mac 7844-E538-0306 FFFF-FF00-0000
[SW1-acl-mac-4000]rule 1 permit
[SW1-acl-mac-4000]quit
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]packet-filter mac 4000 outbound
[SW1-GigabitEthernet1/0/1]quit
```

第二阶段测试：

MAC地址为7844-E538-0306的PC无法PING通服务器

```
h3c_h6lnti
SS620V2-54Q5-GE_1 PC_4 PC_3 PC_2

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

Line con0 is available.

Press ENTER to get started.
<H3C>Feb 21 13:56:31:143 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.
ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
<H3C>Feb 21 13:56:46:949 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 192.168.1.2
: 5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss.
```

除此之外VLAN10另外一个PC可PING通服务器

```
h3c_h6lnti
SS620V2-54Q5-GE_1 PC_4 PC_3 PC_2

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

Line con0 is available.

Press ENTER to get started.
<H3C>Feb 21 13:56:17:668 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.
ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=254 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=254 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=254 time=1.000 ms

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
<H3C>Feb 21 13:56:21:737 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 192.168.1.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/1.200/2.000/0.400 ms.
```

查看MAC ACL匹配的情况:

```
[SW1]dis acl mac all
MAC ACL 4000, 2 rules,
ACL's step is 5
rule 0 deny source-mac 7844-a500-0000 ffff-ff00-0000 (10 times matched)
rule 1 permit (2 times matched)
[SW1]
```

至此，基于二层ACL典型组网配置案例已完成!