

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VLAN 10仅能访问server1，VLAN 20仅能访问server2。R1与SW1运行OSPF路由协议。

配置步骤

- 1、按照网络拓扑图正确配置IP地址
- 2、SW1与R1运行OSPF路由协议
- 3、在SW1配置高级ACL，VLAN 10仅能访问server1，VLAN 20仅能访问server2。

配置关键点

第一阶段调试（基础网络配置）：

```

SW1:
SW1:
sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SW1
[SW1]int loopback 0
[SW1-LoopBack0]ip address 1.1.1.1 32
[SW1-LoopBack0]quit
[SW1]router id 1.1.1.1
[SW1]vlan 10
[SW1-vlan10]quit
[SW1]vlan 20
[SW1-vlan20]quit
[SW1]int vlan 10
[SW1-Vlan-interface10]ip address 172.16.10.1 24
[SW1-Vlan-interface10]quit
[SW1]int vlan 20
[SW1-Vlan-interface20]ip address 172.16.20.1 24
[SW1-Vlan-interface20]quit
[SW1]int gi 1/0/2
[SW1-GigabitEthernet1/0/2]port link-type access
[SW1-GigabitEthernet1/0/2]port access vlan 10
[SW1-GigabitEthernet1/0/2]quit
[SW1]int gi 1/0/3
[SW1-GigabitEthernet1/0/3]port link-type access
[SW1-GigabitEthernet1/0/3]port access vlan 20
[SW1-GigabitEthernet1/0/3]quit
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-mode route
[SW1-GigabitEthernet1/0/1]des
[SW1-GigabitEthernet1/0/1]ip address 10.0.0.1 30
[SW1-GigabitEthernet1/0/1]quit
    
```

```
[SW1]ospf 1 router-id 1.1.1.1
[SW1-ospf-1]area 0.0.0.0
[SW1-ospf-1-area-0.0.0.0]network 10.0.0.1 0.0.0.0
[SW1-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[SW1-ospf-1-area-0.0.0.0]network 172.16.10.0 0.0.0.255
[SW1-ospf-1-area-0.0.0.0]network 172.16.20.0 0.0.0.255
[SW1-ospf-1-area-0.0.0.0]quit
[SW1-ospf-1]quit
[SW1]
```

R1:

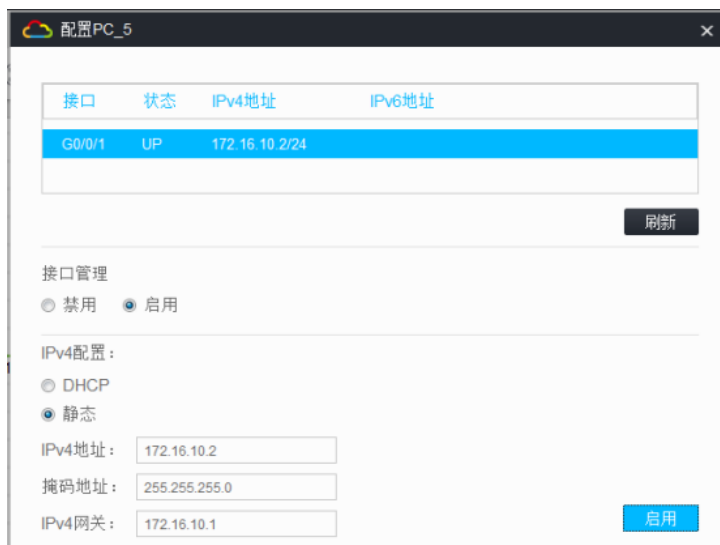
sys

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

```
[H3C]sysname R1
[R1]int gi 0/0
[R1-GigabitEthernet0/0]des
[R1-GigabitEthernet0/0]ip address 10.0.0.2 30
[R1-GigabitEthernet0/0]quit
[R1]int gi 0/1
[R1-GigabitEthernet0/1]ip address 192.168.1.1 24
[R1-GigabitEthernet0/1]quit
[R1]int gi 0/2
[R1-GigabitEthernet0/2]ip address 192.168.2.1 24
[R1-GigabitEthernet0/2]quit
[R1]int loopback 0
[R1-LoopBack0]ip address 2.2.2.2 32
[R1-LoopBack0]quit
[R1]router id 2.2.2.2
[R1]ospf 1 router-id 2.2.2.2
[R1-ospf-1]area 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.0.0.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]quit
[R1-ospf-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	172.16.20.2/24	

刷新

接口管理

禁用 启用

IPv4配置:

DHCP

静态

IPv4地址:

掩码地址:

IPv4网关:

启用

配置PC_3

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:

掩码地址:

IPv4网关:

启用

配置PC_6

接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	192.168.2.2/24	

刷新

接口管理

禁用 启用

IPv4配置:

DHCP

静态

IPv4地址:

掩码地址:

IPv4网关:

启用

```
hcl_r5rgg
SS820V2-54Q5-GE_1 MSK36-20_2 PC_5 PC_4 PC_3
<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=253 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=253 time=4.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=253 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=253 time=2.000 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 = 1.000/2.200/4.000/0.980 ms
<H3C>%Feb 21 09:08:24:133 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 = 1.000/2.200/4.000/0.980 ms.

<H3C>ping 192.168.2.2
Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.2.2: icmp_seq=0 ttl=253 time=3.000 ms
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=3.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=7.000 ms

--- Ping statistics for 192.168.2.2 ---
```

```
hcl_r5rgg
SS820V2-54Q5-GE_1 MSK36-20_2 PC_5 PC_4 PC_3
<H3C>%Feb 21 09:08:45:517 2020 H3C SHELL/S/SHELL_LOGIN: Console logged in from con0.

<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=253 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=253 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=253 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 = 1.000/2.400/3.000/0.800 ms
<H3C>%Feb 21 09:08:52:667 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 = 1.000/2.400/3.000/0.800 ms.

<H3C>ping 192.168.2.2
Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.2.2: icmp_seq=0 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=1.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=2.000 ms
```

```
hcl_r5rgg
SS820V2-54Q5-GE_1 MSK36-20_2 PC_5 PC_4 PC_3
<H3C>%Feb 21 09:09:11:937 2020 H3C SHELL/S/SHELL_LOGIN: Console logged in from con0.

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=253 time=3.000 ms
56 bytes from 172.16.10.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 172.16.10.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 172.16.10.2: icmp_seq=3 ttl=253 time=3.000 ms
56 bytes from 172.16.10.2: icmp_seq=4 ttl=253 time=3.000 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 = 2.000/2.800/3.000/0.400 ms
<H3C>%Feb 21 09:09:16:341 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 = 2.000/2.800/3.000/0.400 ms.

<H3C>ping 172.16.20.2
Ping 172.16.20.2 (172.16.20.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.20.2: icmp_seq=0 ttl=253 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=1 ttl=253 time=3.000 ms
56 bytes from 172.16.20.2: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=4 ttl=253 time=1.000 ms

--- Ping statistics for 172.16.20.2 ---
```

```
hcl_r5rgg
SS820V2-54Q5-GE_1 MSK36-20_2 PC_5 PC_4 PC_3 PC_6
<H3C>ping 172.16.10.1
Ping 172.16.10.1 (172.16.10.1): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.10.1: icmp_seq=0 ttl=254 time=3.000 ms
56 bytes from 172.16.10.1: icmp_seq=1 ttl=254 time=2.000 ms
56 bytes from 172.16.10.1: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 172.16.10.1: icmp_seq=3 ttl=254 time=1.000 ms
56 bytes from 172.16.10.1: icmp_seq=4 ttl=254 time=1.000 ms

--- Ping statistics for 172.16.10.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.600/3.000/0.800 ms
<H3C>%Feb 21 09:10:06:133 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 172.16.10.1
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/1.600/3.000/0.800 ms.

<H3C>ping 172.16.20.2
Ping 172.16.20.2 (172.16.20.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.20.2: icmp_seq=0 ttl=253 time=3.000 ms
56 bytes from 172.16.20.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 172.16.20.2: icmp_seq=3 ttl=253 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=4 ttl=253 time=2.000 ms

--- Ping statistics for 172.16.20.2 ---
```

第二阶段调试（高级ACL关键配置点）：

SW1:

```

[SW1]acl advanced 3000
[SW1-acl-ipv4-adv-3000]rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.1.0 0.0.0.2
55
[SW1-acl-ipv4-adv-3000]rule 1 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.2.0 0.0.0.2
55
[SW1-acl-ipv4-adv-3000]rule 3 deny ip source 172.16.10.0 0.0.0.255 destination 192.168.2.0 0.0.0.25
5
[SW1-acl-ipv4-adv-3000]rule 4 deny ip source 172.16.20.0 0.0.0.255 destination 192.168.1.0 0.0.0.25
5
[SW1-acl-ipv4-adv-3000]quit
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]packet-filter 3000 outbound
[SW1-GigabitEthernet1/0/1]quit

```

第二阶段测试:

VLAN 10的终端能PING通server1, 无法Ping通server2:

```

hcl_r15rgg
SS620V2-54Q5-GE_1 x MSK36-20_2 x PC_5 x PC_4 x PC_3 x PC_6 x
<H3C>Feb 21 09:23:41:210 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.
<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=253 time=4.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=253 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=253 time=4.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=253 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 = 1.000/2.400/4.000/1.356 ms
<H3C>Feb 21 09:23:47:727 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 = 1.000/2.400/4.000/1.356 ms.

<H3C>ping 192.168.2.2
Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
Request time out

```

Vlan 20的终端能PING通server2, PING不通server1:

```

hcl_r15rgg
SS620V2-54Q5-GE_1 x MSK36-20_2 x PC_5 x PC_4 x PC_3 x PC_6 x
Press ENTER to get started.
<H3C>Feb 21 09:25:05:969 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.
ping 192.168.2.2
Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.2.2: icmp_seq=0 ttl=253 time=7.000 ms
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=1.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=2.000 ms

--- Ping statistics for 192.168.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.800/7.000/2.135 ms
<H3C>Feb 21 09:25:10:154 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 192.168.2.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/2.800/7.000/2.135 ms.

<H3C>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
Request time out

```

Server1能PING通VLAN 10的终端, PING不通VLAN 20的终端:

```
hcl_r15rgg
SS820V2-54Q5-GE_1 MSR36-20_2 PC_5 PC_4 PC_3 PC_6
Press ENTER to get started.
<H3C>Feb 21 09:25:57:893 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.
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=253 time=3.000 ms
56 bytes from 172.16.10.2: icmp_seq=1 ttl=253 time=1.000 ms
56 bytes from 172.16.10.2: icmp_seq=2 ttl=253 time=1.000 ms
56 bytes from 172.16.10.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 172.16.10.2: icmp_seq=4 ttl=253 time=2.000 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 = 1.000/1.800/3.000/0.748 ms
<H3C>Feb 21 09:26:02:054 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 = 1.000/1.800/3.000/0.748 ms.

<H3C>ping 172.16.20.2
Ping 172.16.20.2 (172.16.20.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

Server2能PING通VLAN 20的终端，PING不通VLAN 10的终端：

```
hcl_r15rgg
SS820V2-54Q5-GE_1 MSR36-20_2 PC_5 PC_4 PC_3 PC_6
<H3C>ping 172.16.20.2
Ping 172.16.20.2 (172.16.20.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.20.2: icmp_seq=0 ttl=253 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=1 ttl=253 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=3 ttl=253 time=3.000 ms
56 bytes from 172.16.20.2: icmp_seq=4 ttl=253 time=3.000 ms

--- Ping statistics for 172.16.20.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/4.000/1.020 ms
<H3C>Feb 21 09:27:20:694 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 172.16.20.2
: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/
std-dev = 1.000/2.600/4.000/1.020 ms.

<H3C>ping 172.16.10.1
Ping 172.16.10.1 (172.16.10.1): 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 172.16.10.1 ---
```

查看ACL的匹配情况：

```
[SW1]dis acl all
Advanced IPv4 ACL 3000, 4 rules,
ACL's step is 5
 rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 (3 times
matched)
 rule 1 permit ip source 172.16.20.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 (2 times
matched)
 rule 3 deny ip source 172.16.10.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 (15 times m
atched)
 rule 4 deny ip source 172.16.20.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 (10 times m
atched)
[SW1]
```

至此，高级ACL典型组网配置案例已完成！