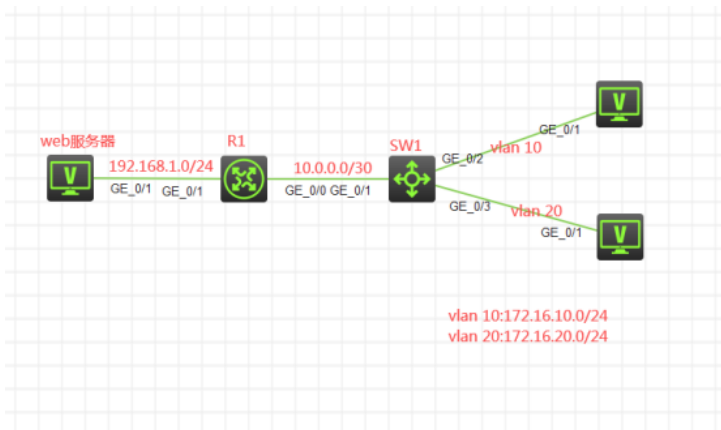


知 基本ACL典型组网配置案例

[ACL](#)[VLAN](#)[OSPF](#)[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模拟器来模拟基本ACL的典型组网配置。在网络拓扑图中已经有了客户机和服务器的标识。R1与SW1运行OSPF路由协议。要求VLAN 20无法访问WEB服务器。

配置步骤

- 1、按照网络拓扑图正确配置IP地址
- 2、R1与SW1运行OSPF路由协议
- 3、SW1配置基本ACL，VLAN 20无法访问WEB服务器

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]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 <connect to R1>
[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:

```

<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname R1
[R1]int gi 0/0
[R1-GigabitEthernet0/0]des <connect to SW1>
[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 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]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_5

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_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

```
hcl_n5rgg
SS620V2-54QS-05_1 MSK36-20_2 PC_5
<H3C>Feb 21 08:46:30:720 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.

<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=254 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=3 ttl=254 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=4 ttl=254 time=1.000 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 = 1.000/1.000/1.000/0.000 ms
<H3C>Feb 21 08:46:37:496 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 = 1.000/1.000/1.000/0.000 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=253 time=3.000 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=2.000 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=2.000 ms
```

```
hcl_n5rgg
SS820V2-54Q5-GE_1  MSB36-20_2  PC_5  PC_4
<H3C>%Feb 21 08:46:56:774 2020 H3C SHELL/5/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=2.000 ms
56 bytes from 172.16.10.2: icmp_seq=2 ttl=254 time=3.000 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=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 = 1.000/2.000/3.000/0.632 ms
<H3C>%Feb 21 08:47:04:1570 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 = 1.000/2.000/3.000/0.632 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=253 time=3.000 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=2.000 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=2.000 ms
```

```
hcl_n5rgg
SS820V2-54Q5-GE_1  MSB36-20_2  PC_5  PC_4  PC_3
<H3C>
<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=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=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 = 2.000/2.400/3.000/0.490 ms
<H3C>%Feb 21 08:47:32:619 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 = 2.000/2.400/3.000/0.490 ms.
\
-
% Unrecognized command found at '^' position.
<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=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=3.000 ms
```

第二阶段调试（基本ACL关键配置点）：

```
[SW1]acl basic 2000
[SW1-acl-ipv4-basic-2000]rule 0 permit source 172.16.10.0 0.0.0.255
[SW1-acl-ipv4-basic-2000]rule 1 deny source 172.16.20.0 0.0.0.255
[SW1-acl-ipv4-basic-2000]quit
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]packet-filter 2000 inbound
[SW1-GigabitEthernet1/0/1]quit
```

第二阶段测试：

VLAN 20的PC无法PING通服务器

```
hcl_n5rgg
SS820V2-54Q5-GE_1  MSB36-20_2  PC_5  PC_4  PC_3
<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=2.000 ms
56 bytes from 172.16.10.2: icmp_seq=2 ttl=254 time=2.000 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=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 = 1.000/1.800/2.000/0.400 ms
<H3C>%Feb 21 08:52:15:954 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 = 1.000/1.800/2.000/0.400 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

--- Ping statistics for 192.168.1.2 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

VLAN 10依然可以PING通服务器：

```
hcl_n5rgg
SS620V2-54Q2-GE_1 MSK36-20_2 PC_5 PC_4 PC_3
<H3C>%Feb 21 08:52:59:968 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.

<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=254 time=3.000 ms
56 bytes from 172.16.20.2: icmp_seq=1 ttl=254 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 172.16.20.2: icmp_seq=3 ttl=254 time=2.000 ms
56 bytes from 172.16.20.2: icmp_seq=4 ttl=254 time=1.000 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 = 1.000/1.800/3.000/0.748 ms
<H3C>%Feb 21 08:53:06:805 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 = 1.000/1.800/3.000/0.748 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=253 time=2.000 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=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=253 time=3.000 ms
```

服务器可以PING通VLAN 10的终端，无法PING通VLAN 20的终端：

```
hcl_n5rgg
SS620V2-54Q2-GE_1 MSK36-20_2 PC_5 PC_4 PC_3
<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=253 time=4.000 ms
56 bytes from 172.16.10.2: icmp_seq=1 ttl=253 time=3.000 ms
56 bytes from 172.16.10.2: icmp_seq=2 ttl=253 time=2.000 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 = 2.000/2.600/4.000/0.800 ms
<H3C>%Feb 21 08:54:12:580 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 = 2.000/2.600/4.000/0.800 ms.

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

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

查看ACL的匹配情况：

```
[SW1]dis acl all
Basic IPv4 ACL 2000, 2 rules,
ACL's step is 5
rule 0 permit source 172.16.10.0 0.0.0.255 (1 times matched)
rule 1 deny source 172.16.20.0 0.0.0.255 (7 times matched)
[SW1:]
```

至此，基本ACL典型组网配置案例已完成！