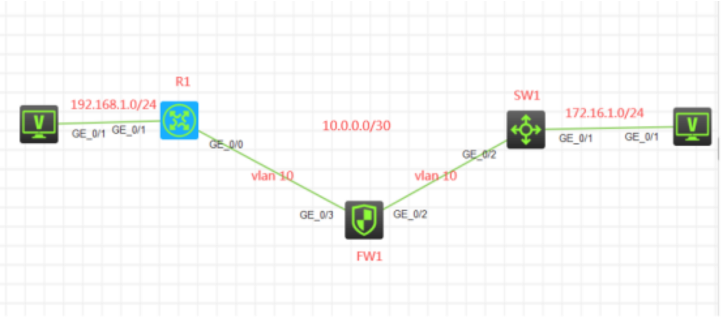
F1060防火墙透明模式典型组网配置案例2（trunk）

透明模式 设备部署方式 H3C模拟器 **韦家宁** 2020-03-24 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器的F1060防火墙来模拟防火墙的透明模式典型组网配置2。为了实现PC之间相互PING通，因此需要在SW1、R1之间通过路由指向来实现路由可达。F1060处在R1、SW1之间，所以将F1060配置为透明模式，采用trunk的方式为R1、SW1透传业务。

配置步骤

1、按照网络拓扑图正确配置IP地址

2、R1与SW1之间运行ospf路由协议

3、将F1060防火墙配置为透明模式，采用trunk的方式为R1、SW1透传业务。

配置关键点

SW1:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SW1
[SW1]vlan 100
[SW1-vlan100]quit
[SW1]int vlan 100
[SW1-Vlan-interface100]ip address 172.16.1.1 24
[SW1-Vlan-interface100]quit
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-type access
[SW1-GigabitEthernet1/0/1]port access vlan 100
[SW1-GigabitEthernet1/0/1]quit
[SW1]vlan 10
[SW1-vlan10]quit
[SW1]int vlan 10
[SW1-Vlan-interface10]ip address 10.0.0.1 30
[SW1-Vlan-interface10]quit
[SW1]int gi 1/0/2
[SW1-GigabitEthernet1/0/2]des <connect to FW1>
[SW1-GigabitEthernet1/0/2]port link-type trunk
[SW1-GigabitEthernet1/0/2]undo port trunk permit vlan 1
[SW1-GigabitEthernet1/0/2]port trunk permit vlan 10
[SW1-GigabitEthernet1/0/2]quit
[SW1]int loopback 0
[SW1-LoopBack0]ip address 1.1.1.1 32
[SW1-LoopBack0]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 172.16.1.0 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 loopback 0
[R1-LoopBack0]ip address 2.2.2.2 32
[R1-LoopBack0]quit
[R1]int gi 0/1
[R1-GigabitEthernet0/1]ip address 192.168.1.1 24
[R1-GigabitEthernet0/1]quit
[R1]vlan 10
[R1-vlan10]quit
[R1]int vlan 10
[R1-Vlan-interface10]ip address 10.0.0.2 30
[R1-Vlan-interface10]quit
[R1]int gi 0/0
[R1-GigabitEthernet0/0]port link-mode bridge
[R1-GigabitEthernet0/0]port link-type trunk
[R1-GigabitEthernet0/0]undo port trunk permit vlan 1
[R1-GigabitEthernet0/0]port trunk permit vlan 10
[R1-GigabitEthernet0/0]quit
[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
```

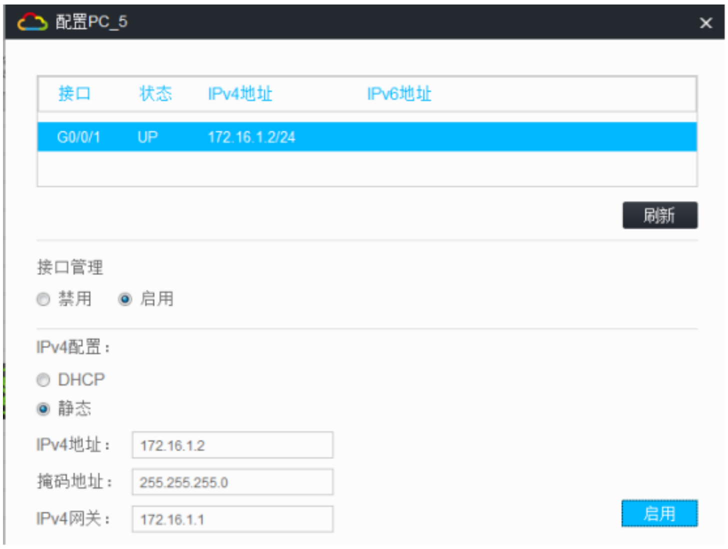
FW1 透明模式配置关键点:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]vlan 10
[FW1-vlan10]quit
[FW1]int range gi 1/0/2 to gi 1/0/3
[FW1-if-range]port link-mode bridge
[FW1-if-range]port link-type trunk
[FW1-if-range]undo port trunk permit vlan 1
[FW1-if-range]port trunk permit vlan 10
[FW1-if-range]quit
[FW1]security-zone name Trust
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/3 vlan 10
[FW1-security-zone-Trust]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/2 vlan 10
[FW1-security-zone-Untrust]quit
[FW1]acl basic 2002
[FW1-acl-ipv4-basic-2002]rule 0 permit source any
[FW1-acl-ipv4-basic-2002]quit
[FW1]
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2002
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2002
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2002
[FW1-zone-pair-security-Trust-Local]quit
[FW1]
```

```
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2002
[FW1-zone-pair-security-Local-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2002
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2002
[FW1-zone-pair-security-Local-Untrust]quit
[FW1]
[FW1]zone-pair security source trust destination trust
[FW1-zone-pair-security-Trust-Trust]packet-filter 2002
[FW1-zone-pair-security-Trust-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination untrust
[FW1-zone-pair-security-Untrust-Untrust]packet-filter 2002
[FW1-zone-pair-security-Untrust-Untrust]quit
```

测试：

所有PC都填写IP地址：



配置PC_5

接口	状态	IPv4地址	IPv6地址
G0/0/1	UP	172.16.1.2/24	

接口管理

○ 禁用 ● 启用

IPv4配置：

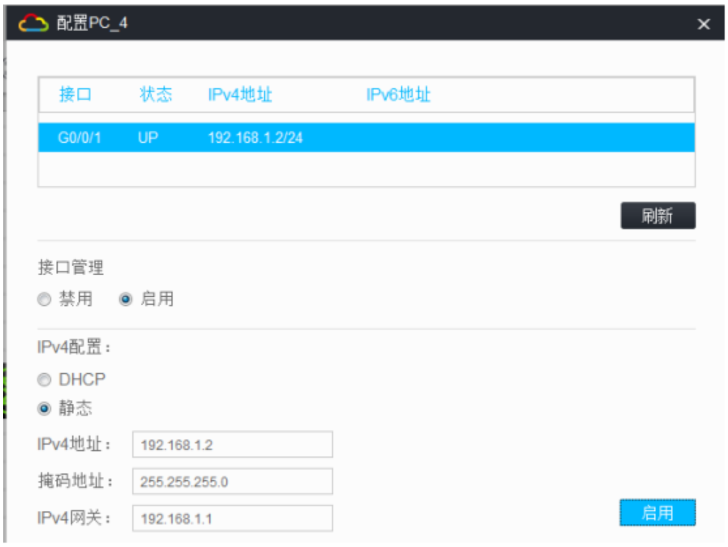
○ DHCP

● 静态

IPv4地址：172.16.1.2

掩码地址：255.255.255.0

IPv4网关：172.16.1.1



配置PC_4

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

接口管理

○ 禁用 ● 启用

IPv4配置：

○ DHCP

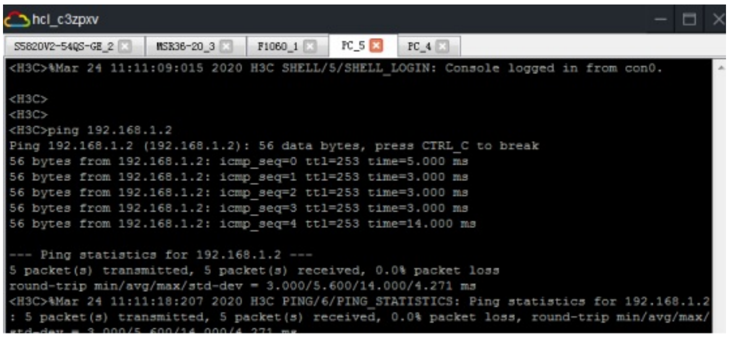
● 静态

IPv4地址：192.168.1.2

掩码地址：255.255.255.0

IPv4网关：192.168.1.1

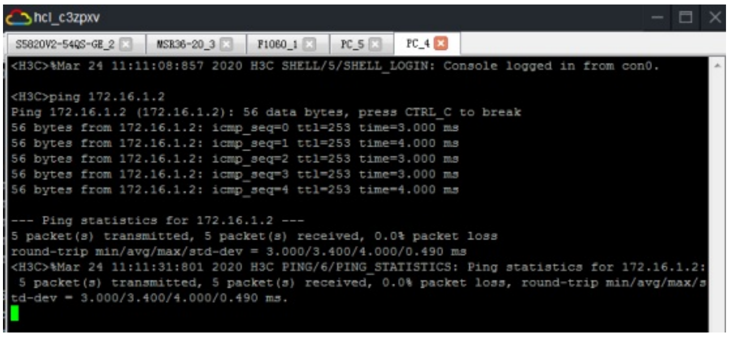
PC之间可以相互PING通：



```
<H3C>%Mar 24 11:11:09:015 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.

<H3C>
<H3C>
<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=5.000 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=14.000 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 = 3.000/5.600/14.000/4.271 ms
<H3C>%Mar 24 11:11:18:207 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 = 3.000/5.600/14.000/4.271 ms
```

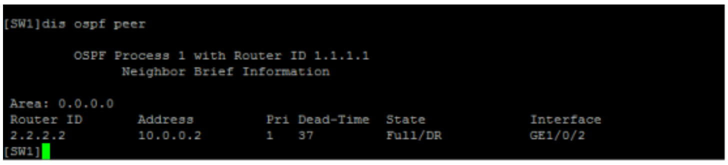


```
<H3C>%Mar 24 11:11:08:857 2020 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.

<H3C>ping 172.16.1.2
Ping 172.16.1.2 (172.16.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.1.2: icmp_seq=0 ttl=253 time=3.000 ms
56 bytes from 172.16.1.2: icmp_seq=1 ttl=253 time=4.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=253 time=3.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=253 time=3.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=253 time=4.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/3.400/4.000/0.490 ms
<H3C>%Mar 24 11:11:31:801 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 172.16.1.2:
 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/s
td-dev = 3.000/3.400/4.000/0.490 ms.
```

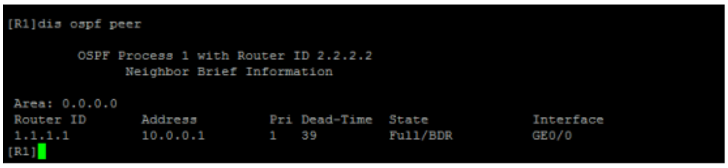
分别查看SW1、R1的OSPF邻居信息：



```
[SW1]dis ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID        Address         Pri Dead-Time  State             Interface
 2.2.2.2          10.0.0.2        1   37         Full/DR           GE1/0/2
[SW1]
```

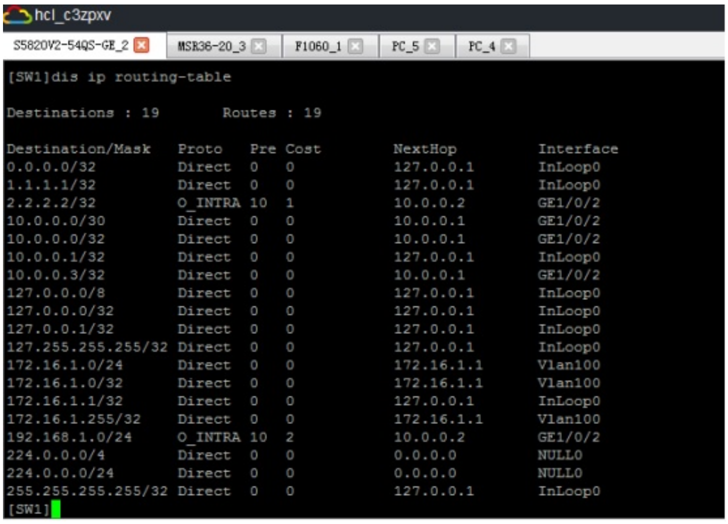


```
[R1]dis ospf peer

         OSPF Process 1 with Router ID 2.2.2.2
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID        Address         Pri Dead-Time  State             Interface
 1.1.1.1          10.0.0.1        1   39         Full/BDR          GE0/0
[R1]
```

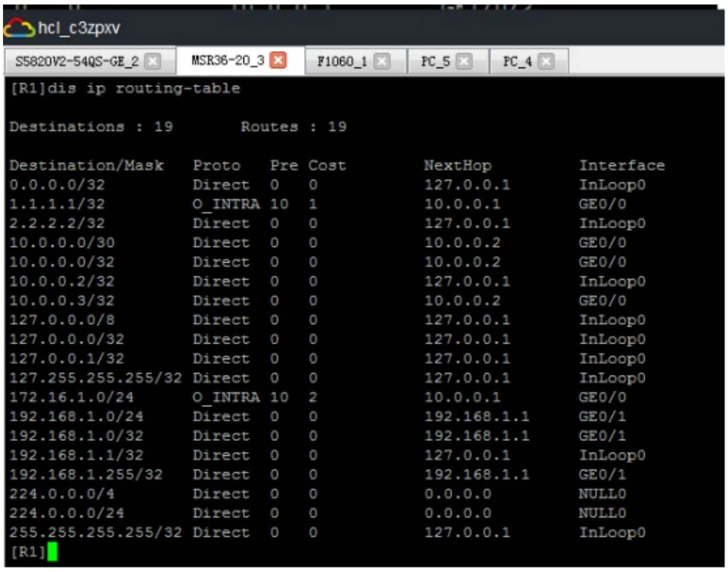
分别查看SW1、R1的路由表：



```
[SW1]dis ip routing-table

Destinations : 19        Routes : 19

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32          Direct  0   0           127.0.0.1       InLoop0
2.2.2.2/32          O_INTRA 10  1           10.0.0.2        GE1/0/2
10.0.0.0/30         Direct  0   0           10.0.0.1        GE1/0/2
10.0.0.0/32         Direct  0   0           10.0.0.1        GE1/0/2
10.0.0.1/32         Direct  0   0           127.0.0.1       InLoop0
10.0.0.3/32         Direct  0   0           10.0.0.1        GE1/0/2
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
172.16.1.0/24       Direct  0   0           172.16.1.1      Vlan100
172.16.1.0/32       Direct  0   0           172.16.1.1      Vlan100
172.16.1.1/32       Direct  0   0           127.0.0.1       InLoop0
172.16.1.255/32     Direct  0   0           172.16.1.1      Vlan100
192.168.1.0/24      O_INTRA 10  2           10.0.0.2        GE1/0/2
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
[SW1]
```

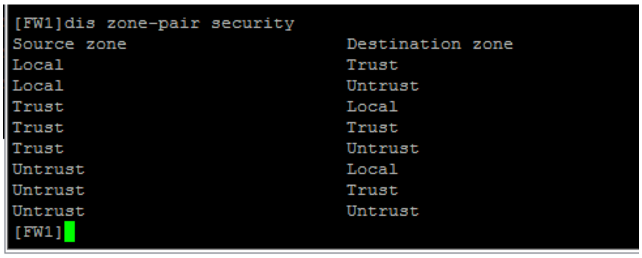


```
[R1]dis ip routing-table

Destinations : 19       Routes : 19

Destination/Mask   Proto   Pre  Cost        NextHop         Interface
0.0.0.0/32         Direct  0    0           127.0.0.1       InLoop0
1.1.1.1/32         O_INTRA 10   1           10.0.0.1        GE0/0
2.2.2.2/32         Direct  0    0           127.0.0.1       InLoop0
10.0.0.0/30        Direct  0    0           10.0.0.2        GE0/0
10.0.0.0/32        Direct  0    0           10.0.0.2        GE0/0
10.0.0.2/32        Direct  0    0           127.0.0.1       InLoop0
10.0.0.3/32        Direct  0    0           10.0.0.2        GE0/0
127.0.0.0/8        Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
172.16.1.0/24      O_INTRA 10   2           10.0.0.1        GE0/0
192.168.1.0/24     Direct  0    0           192.168.1.1     GE0/1
192.168.1.0/32     Direct  0    0           192.168.1.1     GE0/1
192.168.1.1/32     Direct  0    0           127.0.0.1       InLoop0
192.168.1.255/32   Direct  0    0           192.168.1.1     GE0/1
224.0.0.0/4        Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
[R1]
```

查看FW1的zone-pair：



```
[FW1]dis zone-pair security
Source zone                      Destination zone
Local                            Trust
Local                            Untrust
Trust                            Local
Trust                            Trust
Trust                            Untrust
Untrust                          Local
Untrust                          Trust
Untrust                          Untrust
[FW1]
```

温馨提示：如果要实现防火墙的远程登陆管理，建议新增一条链路连接到交换机或者路由器，做带外管理即可。

至此，F1060透明模式典型组网配置案例2（trunk）已完成！