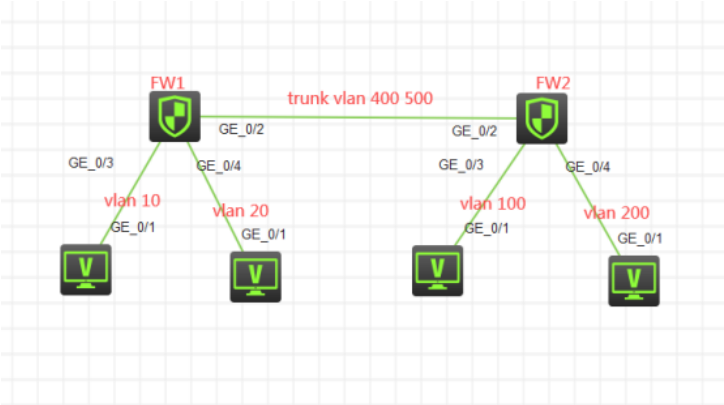
F1060防火墙多VPN实例IBGP典型组网配置案例

设备部署方式 H3C模拟器 **韦家宁** 2020-04-04 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器的F1060防火墙来模拟多VPN实例IBGP典型组网配置。为了实现业务的相互隔离，需要将不同的VLAN绑定到不同的VPN实例中进行业务的互通，因此在本案例引入多实例VPN，将相关的业务进行捆绑。FW1与FW2采用路由模式，都属于AS100，FW1与FW2的互联使用trunk，允许VLAN 400 VLAN 500通过，最终建立多VPN实例IBGP邻居关系，宣告业务网段，使得相同VPN实例的业务能互通，不同VPN实例的业务不能互通。

VPN实例规划如下：

VPN实例名称	RD值	RT值	业务类型	备注
vpn-rt	100:1	100:1	实时业务	
vpn-nrt	200:1	200:1	非实时业务	

IP地址规划如下：

设备名称	接口/VLAN	IP地址	子网掩码位数	所属VPN实例	备注
FW1	VLAN 400	10.0.0.1	30	vpn-rt	互联
	VLAN 500	10.0.0.1	30	vpn-nrt	互联
	VLAN 10	192.168.10.1	24	vpn-rt	
	VLAN 20	192.168.20.1	24	vpn-nrt	
	Loopback 0	1.1.1.1	32	vpn-rt	
	Loopback 1	2.2.2.2	32	vpn-nrt	
FW2	VLAN 400	10.0.0.2	30	vpn-rt	互联
	VLAN 500	10.0.0.2	30	vpn-nrt	互联
	VLAN 100	172.16.10.1	24	vpn-rt	
	VLAN 200	172.16.20.1	24	vpn-nrt	
	Loopback 0	3.3.3.3	32	vpn-rt	
	Loopback 1	4.4.4.4	32	vpn-nrt	

配置步骤

FW1：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
#创建VPN实例，指定RD值、RT值
[FW1]ip vpn-instance vpn-rt
[FW1-vpn-instance-vpn-rt]route-distinguisher 100:1
[FW1-vpn-instance-vpn-rt]vpn-target 100:1
[FW1-vpn-instance-vpn-rt]quit
[FW1]ip vpn-instance vpn-nrt
[FW1-vpn-instance-vpn-nrt]route-distinguisher 200:1
[FW1-vpn-instance-vpn-nrt]vpn-target 200:1
[FW1-vpn-instance-vpn-nrt]quit
[FW1]acl basic 2000
[FW1-acl-ipv4-basic-2000]rule 0 permit source any
[FW1-acl-ipv4-basic-2000]rule 1 permit source any vpn-instance vpn-rt
[FW1-acl-ipv4-basic-2000]rule 2 permit source any vpn-instance vpn-nrt
[FW1-acl-ipv4-basic-2000]quit
```

```
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2000
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2000
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2000
[FW1-zone-pair-security-Trust-Local]quit
[FW1]
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2000
[FW1-zone-pair-security-Local-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2000
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2000
[FW1-zone-pair-security-Local-Untrust]quit
[FW1]
[FW1]zone-pair security source trust destination trust
[FW1-zone-pair-security-Trust-Trust]packet-filter 2000
[FW1-zone-pair-security-Trust-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination untrust
[FW1-zone-pair-security-Untrust-Untrust]packet-filter 2000
[FW1-zone-pair-security-Untrust-Untrust]quit
[FW1]vlan 10
[FW1-vlan10]quit
[FW1]vlan 20
[FW1-vlan20]quit
[FW1]vlan 400
[FW1-vlan400]quit
[FW1]vlan 500
[FW1-vlan500]quit
[FW1]int vlan 10
[FW1-Vlan-interface10]ip binding vpn-instance vpn-rt  //将VLAN绑定到VPN实例
Some configurations on the interface are removed.
[FW1-Vlan-interface10]ip address 192.168.10.1 24
[FW1-Vlan-interface10]quit
[FW1]int vlan 20
[FW1-Vlan-interface20]ip binding vpn-instance vpn-nrt
Some configurations on the interface are removed.
[FW1-Vlan-interface20]ip address 192.168.20.1 24
[FW1-Vlan-interface20]quit
[FW1]int vlan 400
[FW1-Vlan-interface400]ip binding vpn-instance vpn-rt
Some configurations on the interface are removed.
[FW1-Vlan-interface400]des <connect to FW2_vpn-rt>
[FW1-Vlan-interface400]ip address 10.0.0.1 30
[FW1-Vlan-interface400]quit
[FW1]int vlan 500
[FW1-Vlan-interface500]ip binding vpn-instance vpn-nrt
Some configurations on the interface are removed.
[FW1-Vlan-interface500]des <connect to FW2_vpn-nrt>
[FW1-Vlan-interface500]ip address 10.0.0.1 30
[FW1-Vlan-interface500]quit
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]port link-mode bridge
[FW1-GigabitEthernet1/0/3]port link-type access
```

```
[FW1-GigabitEthernet1/0/3]port access vlan 10
[FW1-GigabitEthernet1/0/3]quit
[FW1]int gi 1/0/4
[FW1-GigabitEthernet1/0/4]port link-mode bridge
[FW1-GigabitEthernet1/0/4]port link-type access
[FW1-GigabitEthernet1/0/4]port access vlan 20
[FW1-GigabitEthernet1/0/4]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]port link-mode bridge
[FW1-GigabitEthernet1/0/2]port link-type trunk
[FW1-GigabitEthernet1/0/2]undo port trunk permit vlan 1
[FW1-GigabitEthernet1/0/2]port trunk permit vlan 400 500
[FW1-GigabitEthernet1/0/2]quit
[FW1]security-zone name Trust
[FW1-security-zone-Trust]import interface vlan 10
[FW1-security-zone-Trust]import interface vlan 20
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/3 vlan 10
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/4 vlan 20
[FW1-security-zone-Trust]quit
[FW1]int loopback 0
[FW1-LoopBack0]ip binding vpn-instance vpn-rt
Some configurations on the interface are removed.
[FW1-LoopBack0]ip address 1.1.1.1 32
[FW1-LoopBack0]quit
[FW1]int loopback 1
[FW1-LoopBack1]ip binding vpn-instance vpn-nrt
Some configurations on the interface are removed.
[FW1-LoopBack1]ip address 2.2.2.2 32
[FW1-LoopBack1]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface LoopBack 0
[FW1-security-zone-Untrust]import interface LoopBack 1
[FW1-security-zone-Untrust]import interface vlan 400
[FW1-security-zone-Untrust]import interface vlan 500
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/2 vlan 400 500
[FW1-security-zone-Untrust]quit
[FW1]bgp 100
[FW1-bgp-default]router-id 1.1.1.1
[FW1-bgp-default]ip vpn-instance vpn-rt  //在BGP内绑定VPN实例
[FW1-bgp-default-vpn-rt]peer 10.0.0.2 as-number 100  //指向IBGP邻居
[FW1-bgp-default-vpn-rt]address-family ipv4 unicast
[FW1-bgp-default-ipv4-vpn-rt]peer 10.0.0.2 enable
[FW1-bgp-default-ipv4-vpn-rt]network 192.168.10.0 255.255.255.0
[FW1-bgp-default-ipv4-vpn-rt]network 1.1.1.1 255.255.255.255
[FW1-bgp-default-ipv4-vpn-rt]quit
[FW1-bgp-default-vpn-rt]quit
[FW1-bgp-default]ip vpn-instance vpn-nrt
[FW1-bgp-default-vpn-nrt]peer 10.0.0.2 as-number 100
[FW1-bgp-default-vpn-nrt]address-family ipv4 unicast
[FW1-bgp-default-ipv4-vpn-nrt]peer 10.0.0.2 enable
[FW1-bgp-default-ipv4-vpn-nrt]network 192.168.20.0 255.255.255.0
[FW1-bgp-default-ipv4-vpn-nrt]network 2.2.2.2 255.255.255.255
[FW1-bgp-default-ipv4-vpn-nrt]quit
[FW1-bgp-default-vpn-nrt]quit
[FW1-bgp-default]quit
```

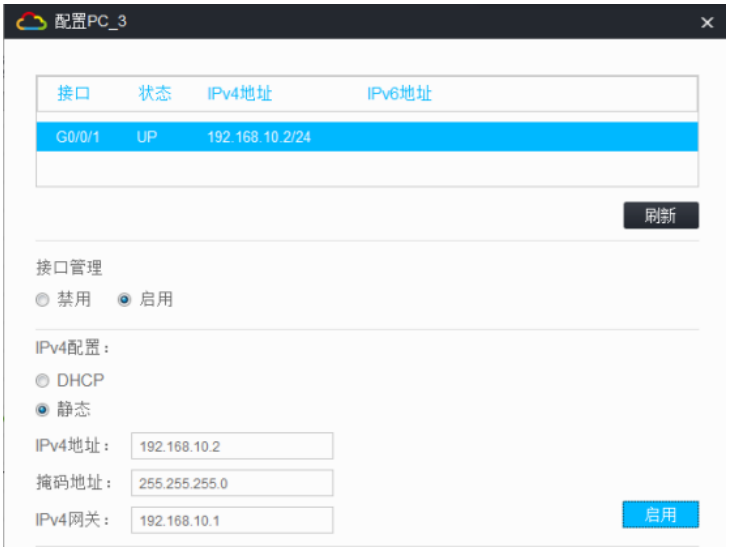
FW2：

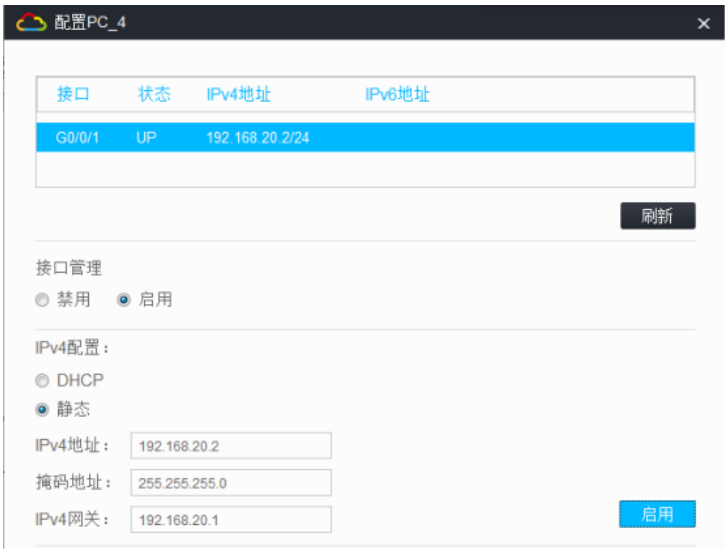
```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW2
[FW2]ip vpn-instance vpn-rt
[FW2-vpn-instance-vpn-rt]route-distinguisher 100:1
[FW2-vpn-instance-vpn-rt]vpn-target 100:1
[FW2-vpn-instance-vpn-rt]quit
```

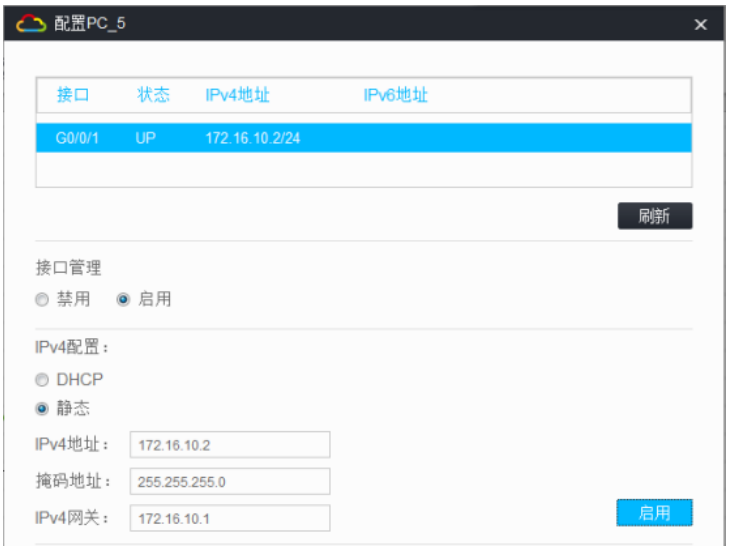
```
[FW2]ip vpn-instance vpn-nrt
[FW2-vpn-instance-vpn-nrt]route-distinguisher 200:1
[FW2-vpn-instance-vpn-nrt]vpn-target 200:1
[FW2-vpn-instance-vpn-nrt]quit
[FW2]acl basic 2000
[FW2-acl-ipv4-basic-2000]rule 0 permit source any
[FW2-acl-ipv4-basic-2000]rule 1 permit source any vpn-instance vpn-rt
[FW2-acl-ipv4-basic-2000]rule 2 permit source any vpn-instance vpn-nrt
[FW2-acl-ipv4-basic-2000]quit
[FW2]zone-pair security source trust destination untrust
[FW2-zone-pair-security-Trust-Untrust]packet-filter 2000
[FW2-zone-pair-security-Trust-Untrust]quit
[FW2]
[FW2]zone-pair security source untrust destination trust
[FW2-zone-pair-security-Untrust-Trust]packet-filter 2000
[FW2-zone-pair-security-Untrust-Trust]quit
[FW2]
[FW2]zone-pair security source trust destination local
[FW2-zone-pair-security-Trust-Local]packet-filter 2000
[FW2-zone-pair-security-Trust-Local]quit
[FW2]
[FW2]zone-pair security source local destination trust
[FW2-zone-pair-security-Local-Trust]packet-filter 2000
[FW2-zone-pair-security-Local-Trust]quit
[FW2]
[FW2]zone-pair security source untrust destination local
[FW2-zone-pair-security-Untrust-Local]packet-filter 2000
[FW2-zone-pair-security-Untrust-Local]quit
[FW2]
[FW2]zone-pair security source local destination untrust
[FW2-zone-pair-security-Local-Untrust]packet-filter 2000
[FW2-zone-pair-security-Local-Untrust]quit
[FW2]
[FW2]zone-pair security source trust destination trust
[FW2-zone-pair-security-Trust-Trust]packet-filter 2000
[FW2-zone-pair-security-Trust-Trust]quit
[FW2]
[FW2]zone-pair security source untrust destination untrust
[FW2-zone-pair-security-Untrust-Untrust]packet-filter 2000
[FW2-zone-pair-security-Untrust-Untrust]quit
[FW2]vlan 100
[FW2-vlan100]quit
[FW2]vlan 200
[FW2-vlan200]quit
[FW2]vlan 400
[FW2-vlan400]quit
[FW2]vlan 500
[FW2-vlan500]quit
[FW2]int vlan 100
[FW2-Vlan-interface100]ip binding vpn-instance vpn-rt
Some configurations on the interface are removed.
[FW2-Vlan-interface100]ip address 172.16.10.1 24
[FW2-Vlan-interface100]quit
[FW2]int vlan 200
[FW2-Vlan-interface200]ip binding vpn-instance vpn-nrt
Some configurations on the interface are removed.
[FW2-Vlan-interface200]ip address 172.16.20.1 24
[FW2-Vlan-interface200]quit
[FW2]int vlan 400
[FW2-Vlan-interface400]ip binding vpn-instance vpn-rt
Some configurations on the interface are removed.
[FW2-Vlan-interface400]ip address 10.0.0.2 30
[FW2-Vlan-interface400]des <connect to FW1_vpn-rt>
[FW2-Vlan-interface400]quit
```

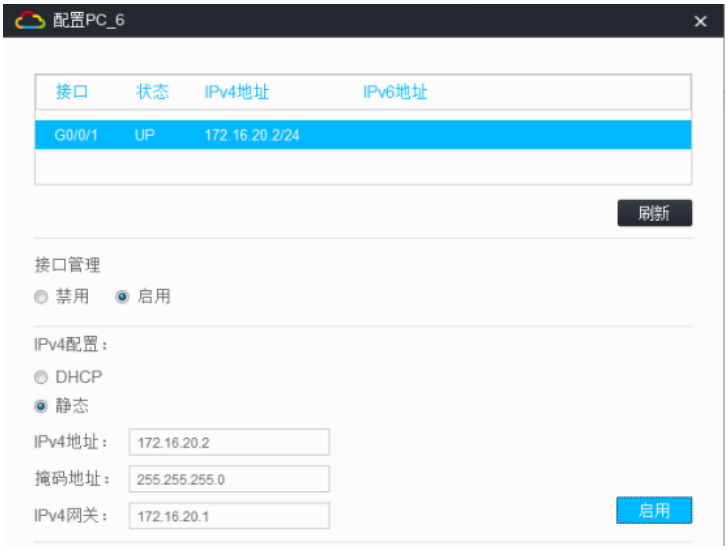
```
[FW2]int vlan 500
[FW2-Vlan-interface500]ip binding vpn-instance vpn-nrt
Some configurations on the interface are removed.
[FW2-Vlan-interface500]ip address 10.0.0.2 30
[FW2-Vlan-interface500]des <connect to FW1_vpn-nrt>
[FW2-Vlan-interface500]quit
[FW2]int loopback 0
[FW2-LoopBack0]ip binding vpn-instance vpn-rt
Some configurations on the interface are removed.
[FW2-LoopBack0]ip address 3.3.3.3 32
[FW2-LoopBack0]quit
[FW2]int loopback 1
[FW2-LoopBack1]ip binding vpn-instance vpn-nrt
Some configurations on the interface are removed.
[FW2-LoopBack1]ip address 4.4.4.4 32
[FW2-LoopBack1]quit
[FW2]int gi 1/0/3
[FW2-GigabitEthernet1/0/3]port link-mode bridge
[FW2-GigabitEthernet1/0/3]port link-type access
[FW2-GigabitEthernet1/0/3]port access vlan 100
[FW2-GigabitEthernet1/0/3]quit
[FW2]int gi 1/0/4
[FW2-GigabitEthernet1/0/4]port link-mode bridge
[FW2-GigabitEthernet1/0/4]port link-type access
[FW2-GigabitEthernet1/0/4]port access vlan 200
[FW2-GigabitEthernet1/0/4]quit
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]port link-mode bridge
[FW2-GigabitEthernet1/0/2]des <connect to FW1>
[FW2-GigabitEthernet1/0/2]port link-type trunk
[FW2-GigabitEthernet1/0/2]undo port trunk permit vlan 1
[FW2-GigabitEthernet1/0/2]port trunk permit vlan 400 500
[FW2-GigabitEthernet1/0/2]quit
[FW2]security-zone name Trust
[FW2-security-zone-Trust]import interface vlan 100
[FW2-security-zone-Trust]import interface vlan 200
[FW2-security-zone-Trust]import interface GigabitEthernet 1/0/3 vlan 100
[FW2-security-zone-Trust]import interface GigabitEthernet 1/0/4 vlan 200
[FW2-security-zone-Trust]quit
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface LoopBack 0
[FW2-security-zone-Untrust]import interface LoopBack 1
[FW2-security-zone-Untrust]import interface GigabitEthernet 1/0/2 vlan 400 500
[FW2-security-zone-Untrust]import interface vlan 400
[FW2-security-zone-Untrust]import interface vlan 500
[FW2-security-zone-Untrust]quit
[FW2]bgp 100
[FW2-bgp-default]router-id 2.2.2.2
[FW2-bgp-default]ip vpn-instance vpn-rt
[FW2-bgp-default-vpn-rt]peer 10.0.0.1 as-number 100
[FW2-bgp-default-vpn-rt]address-family ipv4 unicast
[FW2-bgp-default-ipv4-vpn-rt]peer 10.0.0.1 enable
[FW2-bgp-default-ipv4-vpn-rt]network 172.16.10.0 255.255.255.0
[FW2-bgp-default-ipv4-vpn-rt]network 3.3.3.3 255.255.255.255
[FW2-bgp-default-ipv4-vpn-rt]quit
[FW2-bgp-default-vpn-rt]quit
[FW2-bgp-default]ip vpn-instance vpn-nrt
[FW2-bgp-default-vpn-nrt]peer 10.0.0.1 as-number 100
[FW2-bgp-default-vpn-nrt]address-family ipv4 unicast
[FW2-bgp-default-ipv4-vpn-nrt]peer 10.0.0.1 enable
[FW2-bgp-default-ipv4-vpn-nrt]network 172.16.20.0 255.255.255.0
[FW2-bgp-default-ipv4-vpn-nrt]network 4.4.4.4 255.255.255.255
[FW2-bgp-default-ipv4-vpn-nrt]quit
[FW2-bgp-default-vpn-nrt]quit
```

PC都填写IP地址：

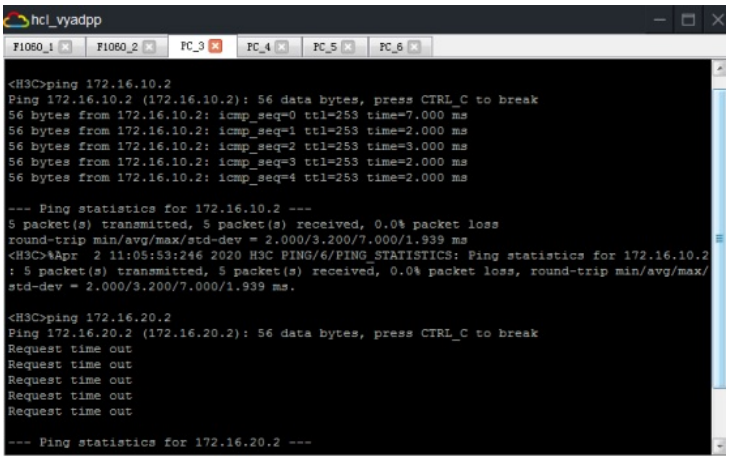

配置PC_3
接口 状态 IPv4地址 IPv6地址
G0/0/1 UP 192.168.10.2/24
刷新
接口管理
禁用 启用
IPv4配置：
DHCP
静态
IPv4地址： 192.168.10.2
掩码地址： 255.255.255.0
IPv4网关： 192.168.10.1
启用

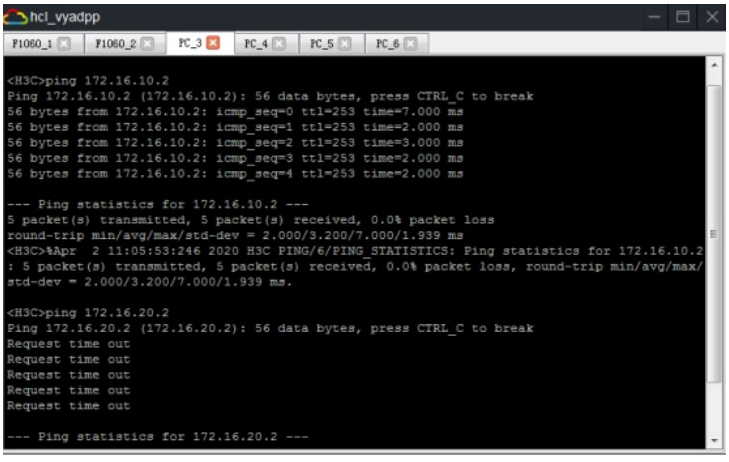

配置PC_4
接口 状态 IPv4地址 IPv6地址
G0/0/1 UP 192.168.20.2/24
刷新
接口管理
禁用 启用
IPv4配置：
DHCP
静态
IPv4地址： 192.168.20.2
掩码地址： 255.255.255.0
IPv4网关： 192.168.20.1
启用

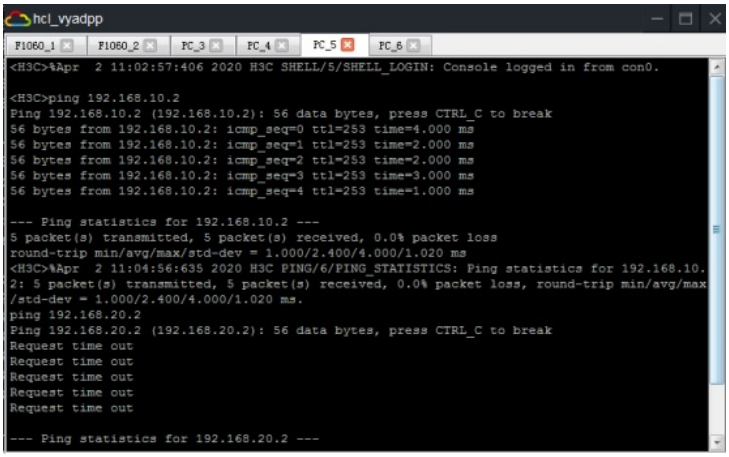

配置PC_5
接口 状态 IPv4地址 IPv6地址
G0/0/1 UP 172.16.10.2/24
刷新
接口管理
禁用 启用
IPv4配置：
DHCP
静态
IPv4地址： 172.16.10.2
掩码地址： 255.255.255.0
IPv4网关： 172.16.10.1
启用

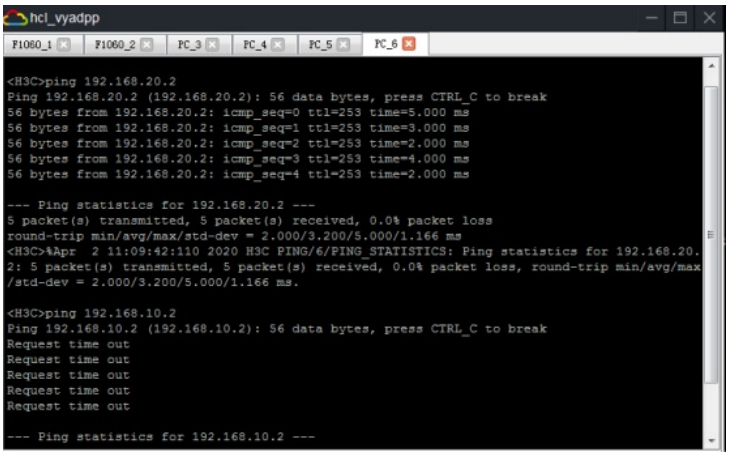


相同VPN实例的业务可以互通，不同VPN实例的业务不可以互通：

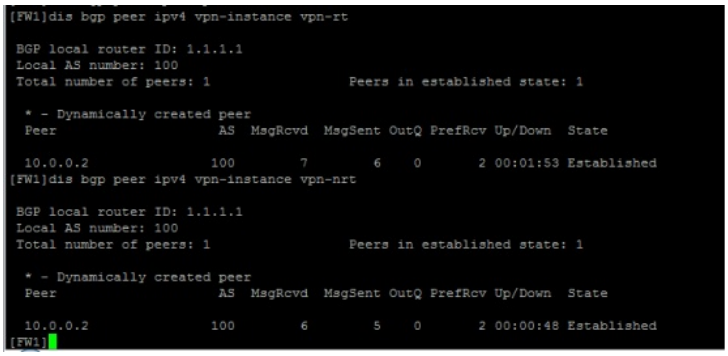




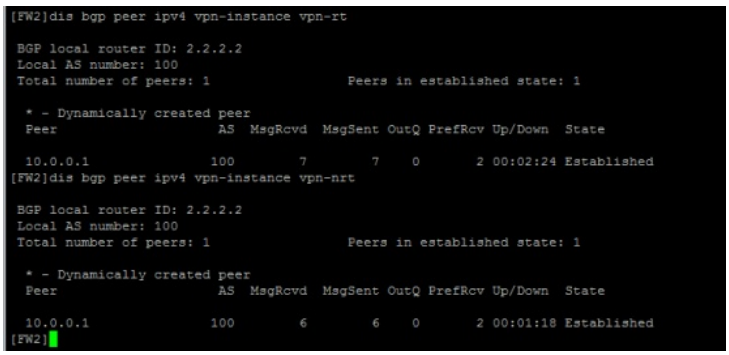




查看FW1的BGP邻居信息：



查看FW2的BGP邻居信息：



至此，F1060多VPN实例BGP典型组网配置案例已完成！

配置关键点