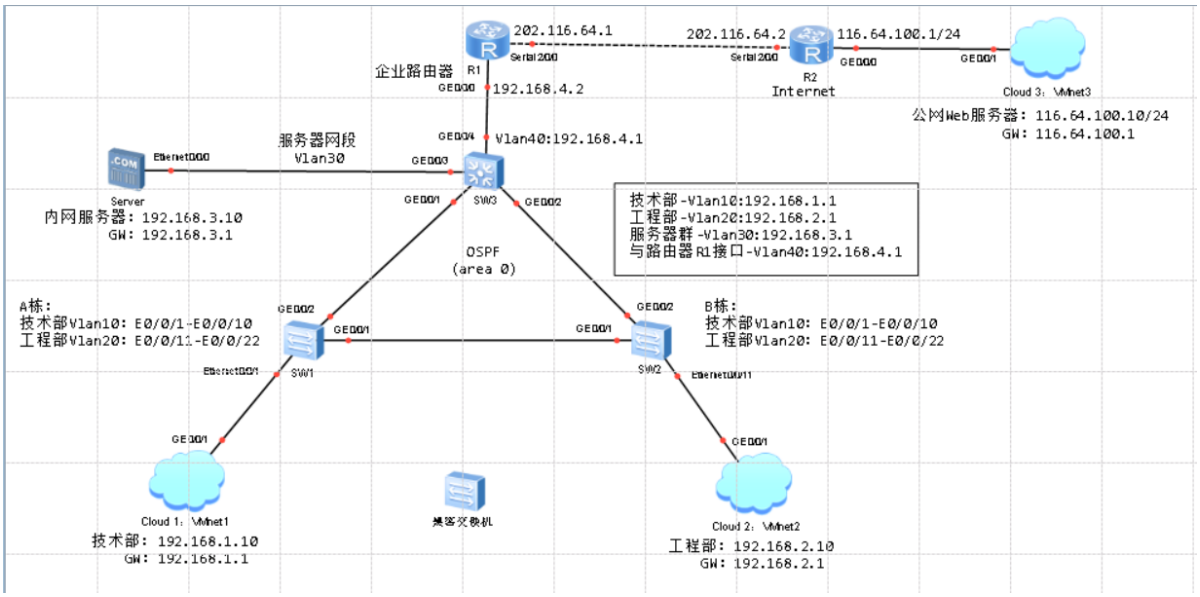
生成树欺骗

基本配置

环境拓扑



基本配置

交换机vlan和端口配置

SW1

```
<Huawei>system-view
[Huawei]sysname SW1
[SW1]undo info-center enable
Info: Information center is disabled.
[SW1]vlan batch 10 20
Info: This operation may take a few seconds. Please wait for a moment...done.
[SW1]stp mode rstp
Info: This operation may take a few seconds. Please wait for a moment...done.

[SW1]port-group 1
[SW1-port-group-1]group
[SW1-port-group-1]group-member e
[SW1-port-group-1]group-member Ethernet 0/0/1 to e
[SW1-port-group-1]group-member Ethernet 0/0/1 to Ethernet 0/0/10
[SW1-port-group-1]port link-type access
[SW1-port-group-1]port default vlan 10
[SW1-port-group-1]quit

[SW1]port-group 2
[SW1-port-group-2]group-member Ethernet 0/0/11 to e0/0/22
[SW1-port-group-2]port link-type access
[SW1-port-group-2]port default vlan 20
[SW1-port-group-2]q

[SW1]port-group 3
```

```
[SW1-port-group-3]group-member g0/0/1 g0/0/2
[SW1-port-group-3]port link-type trunk
[SW1-port-group-3]port trunk allow-pass vlan 10 20
[SW1-port-group-3]q
[SW1]
```

SW2

```
<Huawei>system-view
[Huawei]sysname SW2
[SW2]undo info-center enable
[SW2]vlan batch 10 20
[SW2]stp enable
[SW2]stp mode rstp

[SW2]port-group 1
[SW2-port-group-1]group-member e0/0/1 to e0/0/10
[SW2-port-group-1]port link-type access
[SW2-port-group-1]port default vlan 10
[SW2-port-group-1]q

[SW2]port-group 2
[SW2-port-group-2]group-member e0/0/11 to e0/0/22
[SW2-port-group-2]port link-type access
[SW2-port-group-2]port default vlan 20
[SW2-port-group-2]q

[SW2]port-group 3
[SW2-port-group-3]group-member g0/0/1 g0/0/2
[SW2-port-group-3]port link-type trunk
[SW2-port-group-3]port trunk allow-pass vlan 10 20
[SW2-port-group-3]q
[SW2]
```

SW3

```
<Huawei>
<Huawei>sys
<Huawei>system-view
[Huawei]sysname SW3
[SW3]undo info-center enable
[SW3]vlan batch 10 20 30 40
[SW3]stp enable
[SW3]stp mode rstp
[SW3]stp root primary

[SW3]int g0/0/1
[SW3-GigabitEthernet0/0/1]port link-type trunk
[SW3-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
[SW3-GigabitEthernet0/0/1]q

[SW3]int g0/0/2
[SW3-GigabitEthernet0/0/2]port link-type trunk
[SW3-GigabitEthernet0/0/2]oprt trunk all
[SW3-GigabitEthernet0/0/2]port trunk allow-pass vlan 10 20
```

```
[SW3-GigabitEthernet0/0/2]q

[SW3]int g0/0/3
[SW3-GigabitEthernet0/0/3]port link-type access
[SW3-GigabitEthernet0/0/3]port default vlan 30
[SW3-GigabitEthernet0/0/3]q

[SW3]int g0/0/4
[SW3-GigabitEthernet0/0/4]port link-type trunk
[SW3-GigabitEthernet0/0/4]port trunk allow-pass vlan all
[SW3-GigabitEthernet0/0/4]q

[SW3]int vlanif 10
[SW3-Vlanif10]ip address 192.168.1.1 24
[SW3-Vlanif10]q
[SW3]int vlanif 20
[SW3-Vlanif20]ip address 192.168.2.1 24
[SW3-Vlanif20]q
[SW3]int vlanif 30
[SW3-Vlanif30]ip address 192.168.3.1 24
[SW3-Vlanif30]q
[SW3]int vlanif 40
[SW3-Vlanif40]ip address 192.168.4.1 24
[SW3-Vlanif40]q
[SW3]int g0/0/4
[SW3-GigabitEthernet0/0/4]port trunk pvid vlan 40
[SW3-GigabitEthernet0/0/4]q
[SW3]
```

接口IP与路由协议配置

SW3

```
[SW3]ospf 1
[SW3-ospf-1]area 0
[SW3-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.2.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]q
[SW3-ospf-1]ip route-static 0.0.0.0 0.0.0.0 192.168.4.2
[SW3]
```

R1

```
<Huawei>sys
[Huawei]sysname R1
[R1]undo info-center enable

[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 192.168.4.2 24
[R1-GigabitEthernet0/0/0]q
[R1]

[R1]int s2/0/0
```

```
[R1-Serial2/0/0]ip add 202.116.64.1 24
[R1-Serial2/0/0]q

[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 192.168.4.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]q
[R1-ospf-1]q
[R1]ip route-static 0.0.0.0 0.0.0.0 202.116.64.2
[R1]
```

R2

```
<Huawei>system-view
[Huawei]sysname R2
[R2]undo info-center enable
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 116.64.100.1 24
[R2-GigabitEthernet0/0/0]q
[R2]int s2/0/0
[R2-Serial2/0/0]ip add 202.116.64.2 24
[R2-Serial2/0/0]q
[R2]
```

路由器R1 Easy-IP 配置

R1

```
[R1]acl 2000
[R1-acl-basic-2000]rule permit source 192.168.0.0 0.0.255.255
[R1-acl-basic-2000]q
[R1]int s2/0/0
[R1-Serial2/0/0]nat outbound 2000
[R1-Serial2/0/0]q
[R1]
```

基本配置验证

1.查看SW3生成树与端口详细信息

```
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge          :0    .4c1f-cc32-6eac
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :0    .4c1f-cc32-6eac / 0
CIST RegRoot/IRPC    :0    .4c1f-cc32-6eac / 0
CIST RootPortId      :0.0
BPDU-Protection      :Disabled
CIST Root Type       :Primary root
TC or TCN received   :14
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:19m:39s
Number of TC         :17
Last TC occurred     :GigabitEthernet0/0/4
----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol          :Enabled
 Port Role              :Designated Port
 Port Priority          :128
 Port Cost(Dot1T )      :Config=auto / Active=20000
 Designated Bridge/Port    :0.4c1f-cc32-6eac / 128.1
 Port Edged             :Config=default / Active=disabled
 Point-to-point         :Config=auto / Active=true
 Transit Limit          :147 packets/hello-time
```

2.查看SW3生成树借口简要信息

```
[SW3]display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/4        DESI  FORWARDING      NONE
```

入侵配置

黑客交换机接入与生成树配置

```
<Huawei>
<Huawei>system-view
[Huawei]sysname Hacker
[Hacker]undo info-center enable
[Hacker]stp enable
[Hacker]stp mode rstp
[Hacker]stp priority 0
[Hacker]
```

生成树重新选举与验证

验证黑客交换机选举为根交换机

```
[Hacker]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge          :0     .4c1f-cc1d-1011
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :0     .4c1f-cc1d-1011 / 0
CIST RegRoot/IRPC    :0     .4c1f-cc1d-1011 / 0
CIST RootPortId      :0.0
BPDU-Protection      :Disabled
TC or TCN received   :5
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:2m:16s
Number of TC         :5
Last TC occurred     :Ethernet0/0/2
----[Port1(Ethernet0/0/1)][FORWARDING]----
```

验证SW3交换机为非根交换机

```
[SW3]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge          :0     .4c1f-cc32-6eac
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :0     .4c1f-cc1d-1011 / 220000
CIST RegRoot/IRPC    :0     .4c1f-cc32-6eac / 0
CIST RootPortId      :128.1
BPDU-Protection      :Disabled
CIST Root Type       :Primary root
TC or TCN received   :25
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:3m:39s
Number of TC         :22
Last TC occurred     :GigabitEthernet0/0/1
```

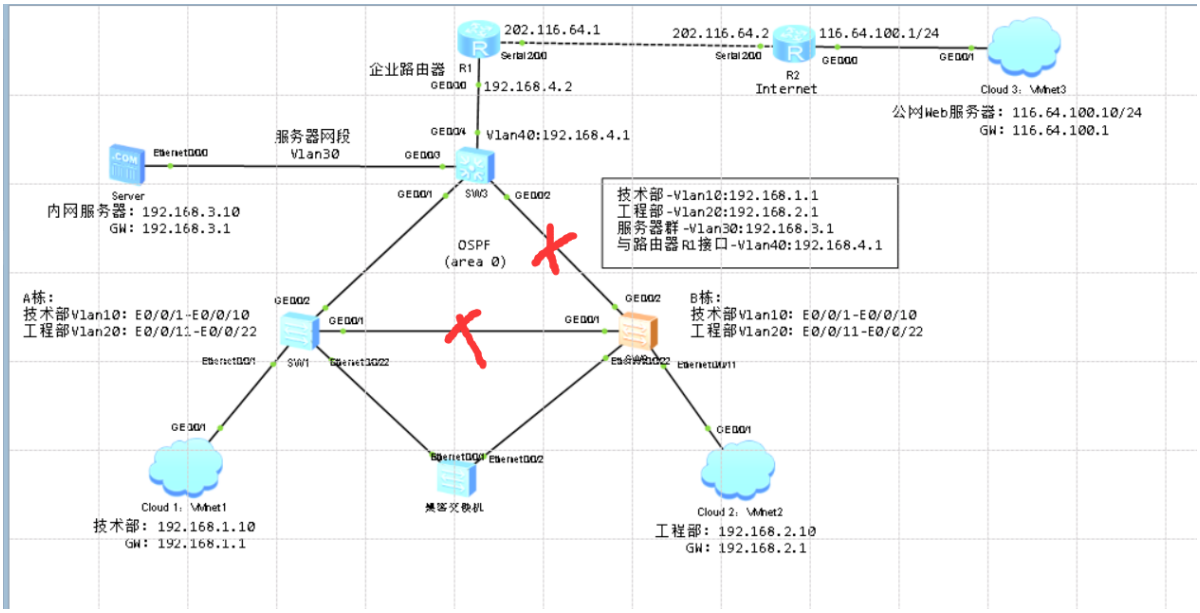
验证SW3阻塞端口与备份链路

```
[SW3]display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/2        ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/4        DESI  FORWARDING      NONE
```

验证SW2阻塞端口与备份链路

```
[SW2]display stp brief
 MSTID  Port                        Role  STP State     Protection
   0    Ethernet0/0/11              DESI  FORWARDING      NONE
   0    Ethernet0/0/22              ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
```

生成树新拓扑结构



防范策略

在交换机SW1和SW2中，将与主机连接的端口设置为边缘端口

SW1

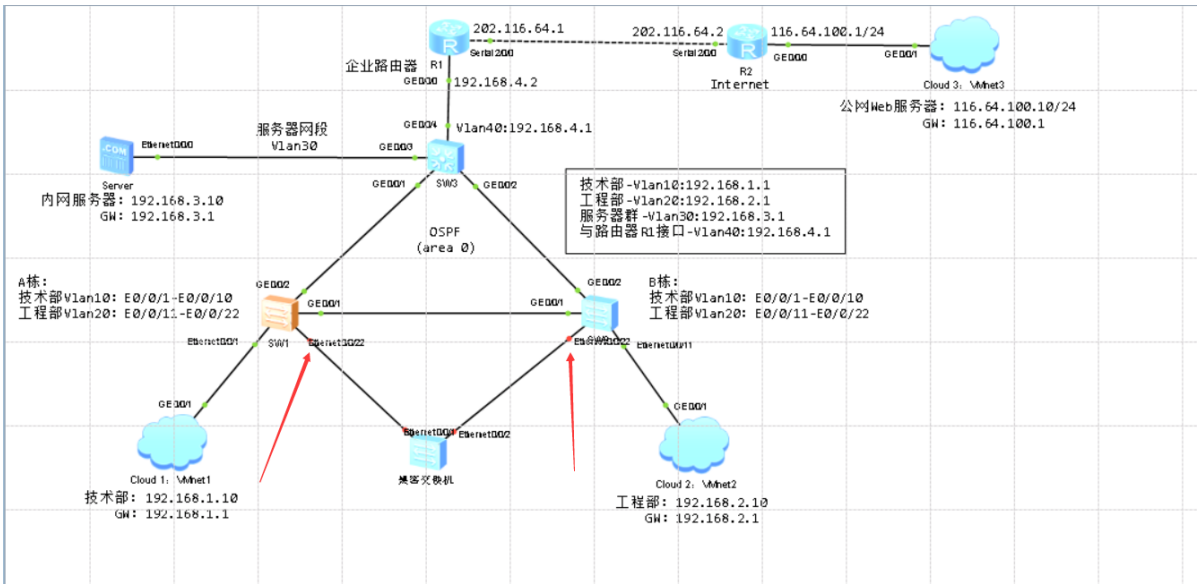
```
[SW1]port-group 1
[SW1-port-group-1]stp edged-port enable
[SW1-port-group-1]quit

[SW1]port-group 2
[SW1-port-group-2]stp edged-port enable
[SW1-port-group-2]q
[SW1]stp bpdu-protection
```

SW2

```
[SW2]port-group 1
[SW2-port-group-1]stp edged-port enable
[SW2-port-group-1]q
[SW2]port-group 2
[SW2-port-group-2]stp edged-port enable
[SW2-port-group-2]q
[SW2]stp bpdu-protection
```

验证

1.开启交换机BPDU保护功能后 SW1和SW2上的E0/0/22端口变红 处于Down状态



2.查看SW3生成树选举结果

```
[SW3]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge          :0    .4c1f-cc32-6eac
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :0    .4c1f-cc32-6eac / 0
CIST RegRoot/IRPC    :0    .4c1f-cc32-6eac / 0
CIST RootPortId      :0.0
BPDU-Protection      :Disabled
CIST Root Type       :Primary root
TC or TCN received   :31
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:3m:21s
Number of TC         :27
Last TC occurred     :GigabitEthernet0/0/2
----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
```