# HCIP-Datacom 分解实验 - 综合实验-2

臧家林制作

## HCIP 综合实验-2

增强分析和配置中小型企业网络的综合能力

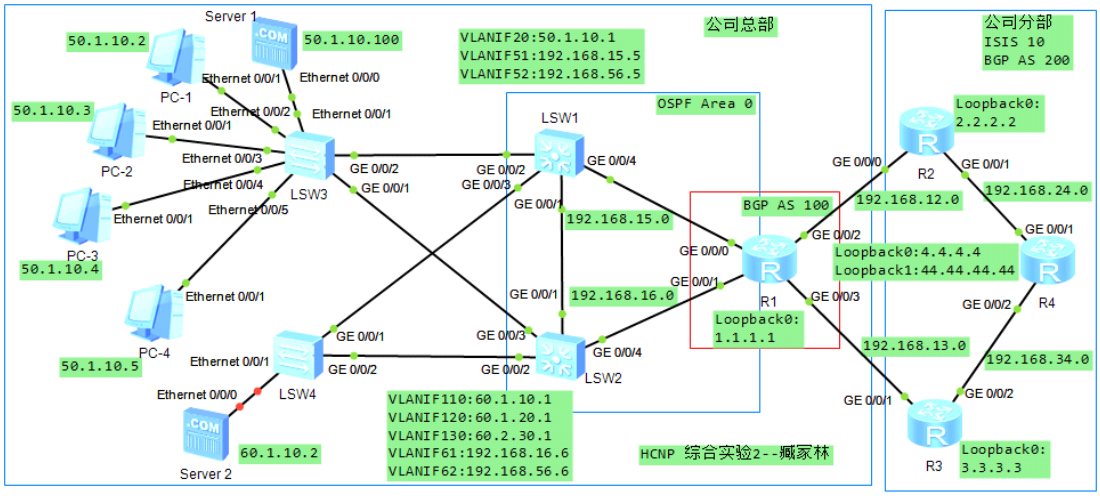
= = = = = = = =

本实验模拟了一个企业网络场景，其中 R1 为公司总部的路由，交换机 SW1、SW2、SW3 、SW4 ，服务器，终端等设备组成了公司总部的园区网，R2、R3、R4 为公司分部的路由器。

公司总部的园区网划分了不同的 VLAN。为了防止二层冗余网络中的环路及提高交换机的防攻击性，每台交换机都需要运行 RSTP 协议，同时还配置 RSTP 保护功能。

在公司总部网络中，R1、SW1、SW2 运行 OSPF 路由协议，并需要通过 OSPF 认证功能来提高安全性。由于种种原因，SW3、SW4 不能运行 OSPF 路由协议，所以网络管理员需要将用户网络段的路由引入 OSPF 进程，在路由引入的同时还需要实现路由聚合。

公司分部网络使用了 IS-IS 路由协议作为 IGP，公司总部网络与公司分部网络之间通过 BGP 路由协议实现互通，这些要求在实现步骤中进行具体的说明。




基本配置

R1:

```
undo terminal monitor
sys
user-interface con 0
idle-timeout 0 0
q
sysname R1
int loop 0
ip add 1.1.1.1 24
int g0/0/0
ip add 192.168.15.1 24
int g0/0/1
ip add 192.168.16.1 24
int g0/0/2
ip add 192.168.12.1 24
int g0/0/3
ip add 192.168.13.1 24
```

q

R2:
undo terminal monitor
sys
user-interface con 0
idle-timeout 0 0
q
sysname R2
int loop 0
ip add 2.2.2.2 24
int g0/0/0
ip add 192.168.12.2 24
int g0/0/1
ip add 192.168.24.2 24
q

R3:
undo terminal monitor
sys
user-interface con 0
idle-timeout 0 0
q
sysname R3
int loop 0
ip add 3.3.3.3 24
int g0/0/1
ip add 192.168.13.3 24
int g0/0/2
ip add 192.168.34.3 24
q

R4:
undo terminal monitor

```
sys
user-interface con 0
idle-timeout 0 0
q
sysname R4
int loop 0
ip add 4.4.4.4 24
int loop 1
ip add 44.44.44.44 24
int g0/0/1
ip add 192.168.24.4 24
int g0/0/2
ip add 192.168.34.4 24
q
```

SW1:

```
undo terminal monitor
sys
user-interface con 0
idle-timeout 0 0
q
sysname SW1
vlan batch 10 20 30 51 52 110 120 130
int vlanif 20
ip add 50.1.10.1 24
int vlanif 51
ip add 192.168.15.5 24
int vlanif 52
ip add 192.168.56.5 24
q
```

SW2:

```
undo terminal monitor
```

```
sys
user-interface con 0
idle-timeout 0 0
q
sysname SW2
vlan batch 10 20 30 61 62 110 120 130
int vlanif 110
ip add 60.1.10.1 24
int vlanif 120
ip add 60.1.20.1 24
int vlanif 130
ip add 60.2.30.1 24
int vlanif 61
ip add 192.168.16.6 24
int vlanif 62
ip add 192.168.56.6 24
q
```

SW3:

```
undo terminal monitor
sys
user-interface con 0
idle-timeout 0 0
q
sysname SW3
vlan batch 10 20 30 110 120 130
```

SW4:

```
undo terminal monitor
sys
user-interface con 0
idle-timeout 0 0
q
```

sysname SW4
vlan batch 10 20 30 110 120 130

========

## 一、交换部分

### 1.接口配置为 Access 、Trunk

配置 SW1 和 SW3 相连接的接口为 access 端口，允许 VLAN 20 通过
配置 SW1 和 SW4 的接口， 配置 SW2 和 SW3 的接口， 配置 SW2 和 SW4 的接口，为 Trunk 端口，允许 VLAN 10、VLAN 20、VLAN 30、VLAN 110、VLAN 120、VLAN 130 通过。

SW1:
int g0/0/2
port link-type access
port default vlan 20
int g0/0/3
port link-type trunk
port trunk allow-pass vlan 10 20 30 110 120 130

SW2
int g0/0/2
port link-type trunk
port trunk allow-pass vlan 10 20 30 110 120 130
int g0/0/3
port link-type trunk
port trunk allow-pass vlan 10 20 30 110 120 130

SW3:
int g0/0/1
port link-type trunk

port trunk allow-pass vlan 10 20 30 110 120 130
int g0/0/2
port link-type access
port default vlan 20

SW4:
int g0/0/1
port link-type trunk
port trunk allow-pass vlan 10 20 30 110 120 130
int g0/0/2
port link-type trunk
port trunk allow-pass vlan 10 20 30 110 120 130
q

在 SW1 和 SW2 上将两个接口划分到相应的 VLAN 中
SW1:
int g0/0/1
port link-type access
port default vlan 52
int g0/0/4
port link-type access
port default vlan 51

SW2:
int g0/0/1
port link-type access
port default vlan 62
int g0/0/4
port link-type access
port default vlan 61

配置完成后在 SW 1 SW2 上查看 VLAN 信息
<SW1>display vlan

```
VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/3(U)      GE0/0/5(D)
                GE0/0/8(D)      GE0/0/9(D)
                GE0/0/12(D)     GE0/0/13(D)
                GE0/0/16(D)     GE0/0/17(D)
                GE0/0/20(D)     GE0/0/21(D)
                GE0/0/24(D)

10   common  TG:GE0/0/3(U)

20   common  UT:GE0/0/2(U)

             TG:GE0/0/3(U)

30   common  TG:GE0/0/3(U)
```

<SW1>display ip int bri

```
Interface                   IP Address/Mask      Physical   Protocol
MEth0/0/1                   unassigned           down       down
NULL0                       unassigned           up         up(s)
Vlanif1                     unassigned           up         down
Vlanif20                    50.1.10.1/24         up         up
Vlanif51                    192.168.15.5/24      up         up
Vlanif52                    192.168.56.5/24      up         up
[SW1]
```

<SW2>display ip int bri

```
Interface                         IP Address/Mask      Physical   Protocol
MEth0/0/1                         unassigned           down       down
NULL0                             unassigned           up         up(s)
Vlanif1                           unassigned           up         down
Vlanif61                          192.168.16.6/24      up         up
Vlanif62                          192.168.56.6/24      up         up
Vlanif110                         60.1.10.1/24         up         up
Vlanif120                         60.1.20.1/24         up         up
Vlanif130                         60.2.30.1/24         up         up
[SW2]
```

Server 2 是属于 VLAN 110 的，要求 Server 2 无论从哪个端口接入 SW4 都必须属于 VLAN 110，为此，基于 MAC 地址将 Server 2 添加进 VLAN 100


SW4:

vlan 110

mac-vlan mac-address 5489-98AC-57B2

int e0/0/1

port hybrid untagged vlan all

mac-vlan enable

查看<SW4>display mac-vlan vlan 110

```
[SW4]display mac-vlan vlan 110
------------------------------------------------------
MAC Address     MASK            VLAN    Priority
------------------------------------------------------
5489-98ac-57b2  ffff-ffff-ffff  110     0

Total MAC VLAN address count: 1
```

========

## 2.Mux VLAN

公司总部园区中，公司员工和公司客户都可以访问公司的服务器，公司内部员工之间也可以互相交流，但与公司客户之间是隔离的，不能够相互访问。公司客户与客户之间不能互访，客户与公司员工也不能互访。这样的需求可以通过 Mux VLAN 来实现：在交换机 SW 3 上，配置 Server 1 所在的 VLAN20 为主 VLAN，配置公司员工 PC1 和 PC2 所在的 VLAN 10 为互通从 VLAN，配置公司客户 PC3 和 PC4 所在的 VLAN 30 为隔离从 VLAN。

SW3:

```
vlan 20
mux-vlan
subordinate group 10
subordinate separate 30

int e0/0/1
port link-type access
port default vlan 20
port mux-vlan enable
int e0/0/2
```

port link-type access
port default vlan 10
port mux-vlan enable
int e0/0/3
port link-type access
port default vlan 10
port mux-vlan enable
int e0/0/4
port link-type access
port default vlan 30
port mux-vlan enable
int e0/0/5
port link-type access
port default vlan 30
port mux-vlan enable
q

配置完成后，查看 Mux VLAN 信息

```
[SW3]dis mux-vlan
Principal Subordinate Type         Interface
------------------------------------------------------------------
20        -           principal    Ethernet0/0/1
20        30          separate     Ethernet0/0/4 Ethernet0/0/5
20        10          group        Ethernet0/0/2 Ethernet0/0/3
------------------------------------------------------------------
```

用 ping 相互测试一下
PC1 能 ping 通 PC2，Server， 但不能 ping 通 PC3 PC4

```
PC>ping 50.1.10.3

Ping 50.1.10.3: 32 data bytes, Press Ctrl_C to break
From 50.1.10.3: bytes=32 seq=1 ttl=128 time=32 ms
From 50.1.10.3: bytes=32 seq=2 ttl=128 time<1 ms
From 50.1.10.3: bytes=32 seq=3 ttl=128 time<1 ms
From 50.1.10.3: bytes=32 seq=4 ttl=128 time<1 ms
From 50.1.10.3: bytes=32 seq=5 ttl=128 time<1 ms
```

=========

## 3.配置 RSTP 协议

为了防止公司总部园区网的二层环路，配置所有的交换机工作在 RSTP 模式。

SW1 为根交换机，SW2 为备份根交换机。

SW1:

stp mode rstp

stp root primary

SW2:

stp mode rstp

stp root secondary

SW3:

stp mode rstp

SW4:

stp mode rstp

配置完成后查看 display stp

```
[SW1]dis stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge          :0    .4c1f-cc53-0798
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-cc53-0798 / 0
CIST RegRoot/IRPC    :0    .4c1f-cc53-0798 / 0
CIST RootPortId      :0.0
BPDU-Protection      :Disabled
CIST Root Type       :Primary root
TC or TCN received   :49
TC count per hello   :0
```

为了提高网络的稳定性，可以配置 RSTP 的根保护功能，使得无论网络发生什么变化，根交换机的角色都不会改变。根保护是指定端口的特性，当端口角色是指定端口时，根保护功能才能生效。

<SW2>display stp brief

```
[SW2]dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/4        DESI  FORWARDING      NONE
```

SW2:
int g0/0/2
stp root-protection
int g0/0/3
stp root-protection

SW2 的 g0/0/4 端口是连接的上行路由器，SW3 SW4 的指定端口连接的是 PC 或服务器，因此这些端口无需配置根保护功能。

如果有攻击者伪造拓扑变化 BPDU 报文来恶意攻击二层网络，则交换机在短时间内会收到大量的拓扑变化 BPDU 报文，这会给交换机的处理工作造成很大的负担。为此，可以通过配置 TC-BPDU 保护功能来解决这个问题。

SW1:

```
stp tc-protection
stp tc-protection threshold 2
```

SW2:

```
stp tc-protection
stp tc-protection threshold 2
```

SW3:

```
stp tc-protection
stp tc-protection threshold 2
```

SW4:

```
stp tc-protection
stp tc-protection threshold 2
```

交换机在单位时间内，允许在收到 TC-BPDU 报文后立即进行地址表项删除操作的最大次数为 2 次。

为了加快收敛速度，将交换机 SW3 和 SW4 连接 PC 服务器的端口配置为边缘端口。

SW3:

```
int e0/0/1
stp edged-port enable
int e0/0/2
stp edged-port enable
```

int e0/0/3
stp edged-port enable
int e0/0/4
stp edged-port enable
int e0/0/5
stp edged-port enable

SW4:
int e0/0/1
stp edged-port enable

交换机的配置工作已经基本完成。

========

## 二、路由部分

### 1.配置 OSPF 路由协议

在 R1 、SW1 和 SW2 上配置 OSPF
R1:
ospf router-id 1.1.1.1
area 0
network 1.1.1.1 0.0.0.0
network 192.168.15.1 0.0.0.0
network 192.168.16.1 0.0.0.0

SW1:
ospf router-id 5.5.5.5
area 0
network 192.168.15.5 0.0.0.0

network 192.168.56.5 0.0.0.0

SW2:
ospf router-id 6.6.6.6
area 0
network 192.168.16.6 0.0.0.0
network 192.168.56.6 0.0.0.0

在 R1 上查看邻居的建立　<R1>display ospf peer brief

```
[R1]display ospf peer brief

    OSPF Process 1 with Router ID 1.1.1.1
         Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id          Interface                       Neighbor id      State
 0.0.0.0          GigabitEthernet0/0/0            5.5.5.5          Full
 0.0.0.0          GigabitEthernet0/0/1            6.6.6.6          Full
 ----------------------------------------------------------------------------
```

## OSPF 路由引入

将 SW1 上的 VLAN 20 所对应的网段作为外部路由引入 OSPF 进程，并进行路由聚合。
将 SW2 上 VLAN 110 、VLAN 120 和 VLAN 130 引入进来，并对 VLAN 110 、VLAN 120 进行路由聚合，VLAN 130 不聚合。
SW1:
ospf
import-route direct
asbr-summary 50.1.0.0 255.255.0.0

SW2:
ospf

import-route direct
asbr-summary 60.1.0.0 255.255.224.0

在 R1 上查看效果

```
50.1.0.0/16   O_ASE    150   2           D    192.168.15.5

60.1.0.0/19   O_ASE    150   2           D    192.168.16.6
```

## OSPF 区域认证

为了提高网络的安全性，R1 SW1 SW2 需要相互通过认证才能交换路由信息。
做 OSPF 的区域认证，简单的明文，密钥为 huawei
R1:
ospf
area 0
authentication-mode simple  huawei

SW1:
ospf
area 0
authentication-mode simple  huawei

SW2:
ospf
area 0
authentication-mode simple  huawei

查看一下 <R1>display ospf brief

```
Area: 0.0.0.0           (MPLS TE not enabled)
Authtype: Simple   Area flag: Normal
SPF scheduled Count: 17
ExChange/Loading Neighbors: 0
Router ID conflict state: Normal
```

========

## 2.配置 IS-IS 路由协议

在公司分部 R2 R3 R4 上配置，为了减少 IS-IS 邻居关系数量和精简链路状态数据库，R2 R3 R4 为 level-2 路由器

R2:

```
isis
network-entity 10.0000.0000.0002.00
is-name R2
is-level level-2
int loo 0
isis enable
int g0/0/1
isis enable
```

R3:

```
isis
network-entity 10.0000.0000.0003.00
is-name R3
is-level level-2
int loo 0
isis enable
int g0/0/2
```

isis enable

R4:
isis
network-entity 10.0000.0000.0004.00
is-name R4
is-level level-2
int loo 0
isis enable
int loo 1
isis enable
int g0/0/1
isis enable
int g0/0/2
isis enable

在 R4 上查看 IS-IS 邻居关系
<R4>display isis peer

```
[R4]dis isis peer

                       Peer information for ISIS(1)

  System Id     Interface          Circuit Id       State HoldTime Type     PRI
------------------------------------------------------------------------------
R2              GE0/0/1            R2.01             Up   8s       L2       64
R3              GE0/0/2            R4.02             Up   27s      L2       64
```

<R4>display ip routing-table

```
 2.2.2.0/24  ISIS-L2 15   10           D   192.168.24.2

 3.3.3.0/24  ISIS-L2 15   10           D   192.168.34.3
```

R4 已经通过 IS-IS 协议获得了 R2 R3 的 loopback 0 网段的路由。

========

## 3.配置 BGP 路由协议

在 R1、R2、R3、R4 上配置 BGP 协议，EBGP 邻居关系采用直连物理接口来建立，IBGP 邻居关系采用 loopback 0 接口来建立。

R1:

```
bgp 100
router-id 1.1.1.1
peer 192.168.12.2 as-number 200
peer 192.168.13.3 as-number 200
```

R2:

```
bgp 200
router-id 2.2.2.2
peer 192.168.12.1 as-number 100
peer 4.4.4.4 as-number 200
peer 4.4.4.4 connect-interface LoopBack 0
peer 4.4.4.4 next-hop-local
peer 3.3.3.3 as-number 200
peer 3.3.3.3   connect-interface LoopBack 0
peer 3.3.3.3   next-hop-local
```

R3:

```
bgp 200
router-id 3.3.3.3
```

peer 192.168.13.1 as-number 100
peer 4.4.4.4 as-number 200
peer 4.4.4.4 connect-interface LoopBack 0
peer 4.4.4.4 next-hop-local
peer 2.2.2.2 as-number 200
peer 2.2.2.2  connect-interface LoopBack 0
peer 2.2.2.2  next-hop-local

R4:
bgp 200
router-id 4.4.4.4
peer 2.2.2.2 as-number 200
peer 2.2.2.2 connect-interface LoopBack 0
peer 3.3.3.3 as-number 200
peer 3.3.3.3 connect-interface LoopBack 0

在 R4 上查看 BGP 邻居关系
<R4>display bgp peer

```
2.2.2.2         4          200        2        2     0 00:00:01 Established
 0
3.3.3.3         4          200        2        2     0 00:00:01 Established
```

## 路由引入

为了让公司分部知道公司总部网络的路由，在 R1 上将 OSPF 引入 BGP 进程
R1：
bgp 100
import-route ospf 1

在 R2 上查看 IP 路由表<R2>display ip routing-table

公司总部不希望公司分部访问 60.2.30.0/24 网段，因为这是总部财务部门所属的网段，所以公司总部的网络管理员决定在 R1 上使用路由策略在引入 OSPF 路由时过滤掉这个网段的路由。
R1:
acl 2000
rule permit source 60.2.30.0 0.0.0.255
route-policy 10 deny node 1
if-match acl 2000
route-policy 10 permit node 2
bgp 100
import-route ospf 1 route-policy 10

在 R4 上查看一下
<R4>display ip routing-table
可以看到 R4 已经学习不到关于 60.2.30.0/24 这个网段的路由了

```
 44.44.44.0/24  Direct  0    0           D   44.44.44.44
44.44.44.44/32  Direct  0    0           D   127.0.0.1
   50.1.0.0/16  IBGP    255  2          RD   2.2.2.2
1
   60.1.0.0/19  IBGP    255  2          RD   2.2.2.2
1
  127.0.0.0/8   Direct  0    0           D   127.0.0.1
  127.0.0.1/32  Direct  0    0           D   127.0.0.1
92.168.15.0/24  IBGP    255  0          RD   2.2.2.2
1
```

为了能将公司分部的路由信息通告给公司总部，在 R2 和 R3 上将 IS-IS 路由引入到 BGP 协议
R2:
bgp 200
import-route isis 1

R3:
bgp 200
import-route isis 1

在 R1 上查看路由表
<R1>display ip routing-table
R1 通过 BGP 接收到了公司分部网络的路由

总部交换机 SW1 和 SW2 由于没有运行 BGP 路由协议，所以无法获得公司分部网络的路由。为些，可以 R1 上通过 OSPF 非强制方式下发缺省路由，SW1 和 SW2 通过该缺省路由来访问公司分部网络。OSPF 非强制下发缺省路由的条件是，IP 路由表中存在非 OSPF 进程的缺省路由。因此，可以在 R2 和 R3 上配置 BGP 下发缺省路由给 R1，使 R1 的路由表中存在一条来自 BGP 的缺省路由。
R1:
ospf
default-route-advertise

R2:
bgp 200
peer 192.168.12.1 default-route-advertise

R3:

bgp 200
peer 192.168.13.1 default-route-advertise

在 SW1 SW2 上查看

<SW1>display ip routing-table

```
[SW1-ospf-1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   192.168.15.1    Vlanif51
        1.1.1.1/32  OSPF    10   1           D   192.168.15.1    Vlanif51
       50.1.10.0/24 Direct  0    0           D   50.1.10.1       Vlanif20
       50.1.10.1/32 Direct  0    0           D   127.0.0.1       Vlanif20
       60.1.0.0/19  O_ASE   150  2           D   192.168.56.6    Vlanif52
```