Index

CCNP Lab Manual

Building Scalable Cisco Internetworks

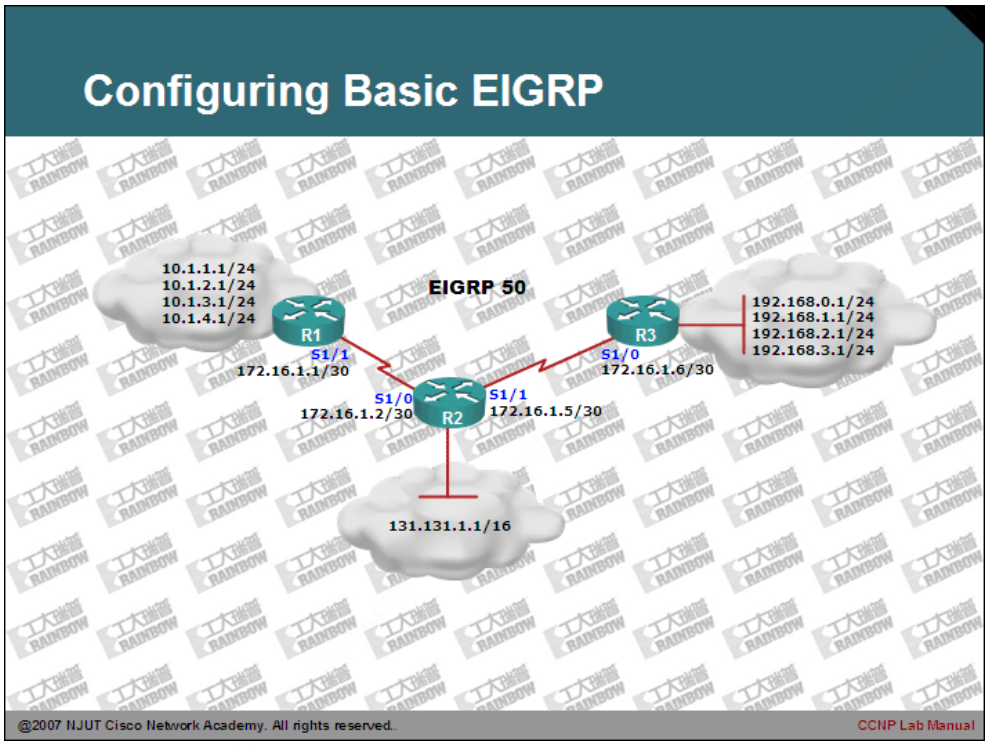
CCNP Lab Manual

Lab 1. Configuring Basic EIGRP

实验目的：

1、掌握 EIGRP 的基本配置。
2、掌握 EIGRP 的通配符掩配置方法。
3、掌握 EIGRP 的自动汇总特性，以及如何关闭自动汇总。
4、掌握 EIGRP 的手工汇总。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 ping 命令确认各路由器的直连口的互通性。

2、在三台路由配置 EIGRP 自治系统编号为 50。

3、登录到 R2 路由器，作如下配置（其它路由器参照其进行配置）：

```
R2#configure terminal
R2(config-if)#router eigrp 50
R2(config-router)#network 172.16.0.0
R2(config-router)#network 131.131.0.0
R2(config-router)#exit
```

批注 [stanley1]: 默认情况下，EIGRP 在配置路由器时，可以直接 network 主类网络号。
此处配置，可以同时将 R2 路由器两个串口直接加入到 EIGRP 的路由进程中。

4、在任意一台路由器上观察 EIGRP 的邻居关系：

```
R2#show ip eigrp 50 neighbors
IP-EIGRP neighbors for process 50
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   172.16.1.6              Se1/1             13 00:00:37  436  2616  0  2
0   172.16.1.1              Se1/0             13 00:02:34  736  4416  0  4
```

批注 [stanley2]: 查看 eigrp 50 自治系统的邻居

其中：列 H 指出邻居学习的顺序,Address 指出邻居地址，Interface 指出邻居所在本地接口。

5、在任意一台路由器上查看路由器，确认路由：

```
R2#show ip route
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.4/30 is directly connected, Serial1/1
D       172.16.0.0/16 is a summary, 00:06:33, Null0
C       172.16.1.0/30 is directly connected, Serial1/0
D    192.168.4.0/24 [90/2297856] via 172.16.1.6, 00:04:39, Serial1/1
D    10.0.0.0/8 [90/2297856] via 172.16.1.1, 00:06:34, Serial1/0
C    131.131.0.0/16 is directly connected, Loopback0
D    192.168.0.0/24 [90/2297856] via 172.16.1.6, 00:04:39, Serial1/1
D    192.168.1.0/24 [90/2297856] via 172.16.1.6, 00:04:39, Serial1/1
D    192.168.2.0/24 [90/2297856] via 172.16.1.6, 00:04:39, Serial1/1
D    192.168.3.0/24 [90/2297856] via 172.16.1.6, 00:04:39, Serial1/1
R2#
```

批注 [stanley3]: EIGRP 会自动的为可汇总的子网生成一条指向 null0 口的路由。
其目的：
1.汇总路由
2.避免路由黑洞

批注 [stanley4]:
90 为 EIGRP 的内部管理距离
2297856 为 EIGRP 计算的度量(FD)

6、在 R1 路由器上使用更简洁的查看关于 EIGRP 的路由命令：

```
R2#show ip route eigrp

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:10:09, Null0
```

```
D    192.168.4.0/24 [90/2297856] via 172.16.1.6, 00:08:14, Serial1/1
D    10.0.0.0/8 [90/2297856] via 172.16.1.1, 00:10:10, Serial1/0
D    192.168.0.0/24 [90/2297856] via 172.16.1.6, 00:08:14, Serial1/1
D    192.168.1.0/24 [90/2297856] via 172.16.1.6, 00:08:14, Serial1/1
D    192.168.2.0/24 [90/2297856] via 172.16.1.6, 00:08:14, Serial1/1
D    192.168.3.0/24 [90/2297856] via 172.16.1.6, 00:08:14, Serial1/1
R2#
```

批注 [stanley5]：R1 路由器的自动汇总的路由。

7、我们注意到在 R2 路由器上有一条指向 s1/0 口的 10.0.0.0/8 的汇总路由，这是 EIGRP 路由协议自动汇总的特性体现。可以使用 no auto-summary 命令关闭。如下：

```
R1(config)
R1(config)#router eigrp 50
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#
```

批注 [stanley6]：关于 EIGRP 的自动汇总特性。

随后在 R2 上观察路由表的变化，如下显示：

```
R2#show ip route eigrp
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:07:26, Null0
D    192.168.4.0/24 [90/2297856] via 172.16.1.6, 00:05:09, Serial1/1
     10.0.0.0/24 is subnetted, 4 subnets
D       10.1.3.0 [90/2297856] via 172.16.1.1, 00:02:31, Serial1/0
D       10.1.2.0 [90/2297856] via 172.16.1.1, 00:02:31, Serial1/0
D       10.1.1.0 [90/2297856] via 172.16.1.1, 00:02:31, Serial1/0
D       10.1.4.0 [90/2297856] via 172.16.1.1, 00:02:31, Serial1/0
D    192.168.0.0/24 [90/2297856] via 172.16.1.6, 00:05:09, Serial1/1
D    192.168.1.0/24 [90/2297856] via 172.16.1.6, 00:05:09, Serial1/1
D    192.168.2.0/24 [90/2297856] via 172.16.1.6, 00:05:09, Serial1/1
D    192.168.3.0/24 [90/2297856] via 172.16.1.6, 00:05:09, Serial1/1
R2#
```

批注 [stanley7]：当关闭了自动汇总后，R2 可以看到明细路由。

7、EIGRP 也可以进行手工地址总结。手工地址总结，可以有效的减少路由表的大小。比如在 R2 上的路由中关于 R3 的 192.168.*.*的网络显示为四条具体路由，可以在 R3 上进行如下配置，减少路由通告条目。

```
R3(config)#interface serail 1/0
R3(config-if)#ip summary eigrp 50 192.168.0.0 255.255.252.0
R3(config-if)#exit
```

8、观察 R2 路由器的路由表：

```
R2#show ip route eigrp
.........
```

```
D       10.1.1.0 [90/2297856] via 172.16.1.1, 00:02:31, Serial1/0
D       10.1.4.0 [90/2297856] via 172.16.1.1, 00:02:31, Serial1/0
D    192.168.0.0/22 [90/2297856] via 172.16.1.6, 00:05:09, Serial1/1
 .........
```

批注 [stanley8]：显示为一条汇总路由。有效的减少路由表的大小。

9、在 R2 上使用通配符掩码进行配置 EIGRP：

```
R2(config)#no router eigrp 50
R2(config)#router eigrp 50
R2(config-router)#network 172.16.1.0 0.0.0.3
R2(config-router)#network 131.131.0.0
R2(config-router)#exit
```

批注 [stanley9]：使用通配符掩码，可以很好的控制，哪些接口加入到 EIGRP 的进程中工作。否则可能需要使用 passive-interface 命令进行了设置。
此处仅将 s1/0 接口加入到 eigrp 中，所以 R2 的 s1/1 接口，和 R3 的路由不会被转发给 R1.

10、在 R2 确认邻居，此处仅发现与 R1 建立了邻居关系。

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 50
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   172.16.1.1              Se1/0             12 00:04:57 1510  5000  0  5
```

11、查看 R1 的路由表，进行确认所学习到的路由。

```
R1#show ip route eigrp
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:02:55, Null0
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:02:55, Null0
D    131.131.0.0/16 [90/2297856] via 172.16.1.2, 00:00:06, Serial1/1
R1#
```

批注 [stanley10]：由于采用通配符掩码，进行选择性的配置，所以 R1 仅学习到 131.131.0.0/16 的路由条目。无法学习到 R3 的直接路由。

12、实验完成。

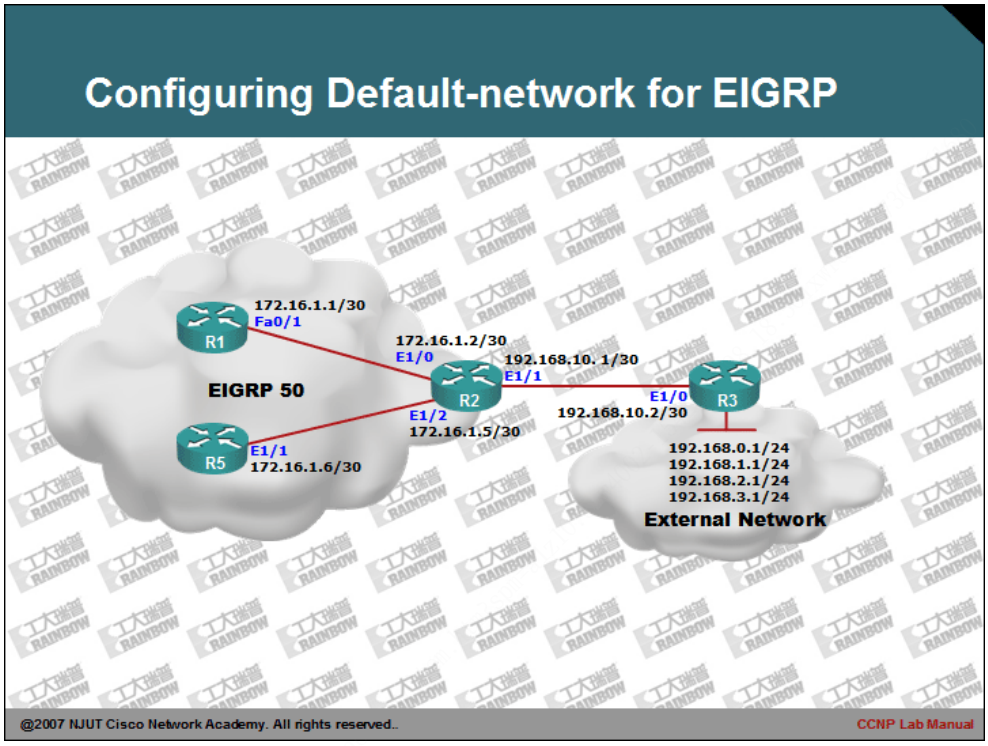
CCNP Lab Manual

Lab 2. Configuring Default-network for EIGRP

实验目的：

1、掌握通过 ip default-network 命令配置 EIGRP 默认网络。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 R3 路由器用于模拟外部网络，也可以把其假想为 Internet 网络，并且在 R3 上配置一条默认用于，以便路由来自于 EIGRP 内部网络的数据包。

```
R3(config)#
R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.1
R3(config)#
```

批注 [stanley11]: 配置此条路由到达EIGRP内部网络。

3、配置 R1、R2 和 R5 路由器的 EIGRP 路由协议，配置如下所示：

```
R1(config)#router eigrp 50
R1(config-router)#network 172.16.0.0
R1(config-router)#exit
```

```
R5(config)#router eigrp 50
R5(config-router)#network 172.16.0.0
R5(config-router)#exit
```

```
R2(config)#router eigrp 50
R2(config-router)#network 172.16.0.0
R2(config-router)#exit
```

4、在 R2 上查看 EIGRP 的邻居，确认 EIGRP 正常运行：

```
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 50
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq Type
                                            (sec)         (ms)       Cnt Num
1   172.16.1.6              Et1/2             11 00:00:54    1   3000  0  2
0   172.16.1.1              Et1/0             12 00:00:54    1   3000  0  2
```

5、在 R2 上配置静态默认路由，用于到达外部网络，配置如下：

```
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
R2(config)#
R2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/43/92 ms
R2#
```

批注 [stanley12]: R2 通过此路由可以访问到外部网络。

批注 [stanley13]: 测试静态默认路由的有效性。

6、路由器 R2 作为企业的出口路由器，由于其配置了静态路由，因此其可以直接

访问外部，但是内部的 R1 和 R5 路由器由于缺少路由，因此无法访问外网。下面显示了 R1 路由器的路由表和其向外部发起 ping 的访问结果：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.1.4 [90/284160] via 172.16.1.2, 00:06:40, FastEthernet0/1
C       172.16.1.0 is directly connected, FastEthernet0/1
R1#
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

批注 [stanley14]： 路由表中显示出 R1 没有外部网络路由。

批注 [stanley15]： 由于 R1 缺少到达外部网络路由，因此 R1 无法访问外部网络。

```
R5#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.4 is directly connected, Ethernet1/1
D       172.16.1.0 [90/307200] via 172.16.1.5, 00:12:15, Ethernet1/1
R5#
R5#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R5#
```

批注 [stanley16]： 内部路由器 R5 也遇到了相同的问题。

7、为了解决问题，只需要在 R1 和 R5 路由器上配置一条指向 R2 路由器的静态默认路由即可，如下所示：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
R1(config)#exit
R1#show ip route

Gateway of last resort is 172.16.1.2 to network 0.0.0.0
```

```
     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.1.4 [90/284160] via 172.16.1.2, 00:09:19, FastEthernet0/1
C       172.16.1.0 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.16.1.2
R1#
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/71/92 ms
R1#
```

批注 [stanley17]： 为R1添加一条到达外网静态默认路由。

批注 [stanley18]： 由于已经此时配置了默认路由，所以此时R1可以访问到外部网络。

```
R5(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.5
R5(config)#exit
R5#
R5#show ip route

Gateway of last resort is 172.16.1.5 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.4 is directly connected, Ethernet1/1
D       172.16.1.0 [90/307200] via 172.16.1.5, 00:13:57, Ethernet1/1
S*   0.0.0.0/0 [1/0] via 172.16.1.5
R5#
R5#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/53/64 ms
R5#
```

8、根据上面配置，其实只需要给内部路由器配置默认路由指向出口路由器 R2 即可解决外部网络无法访问的问题。但是**如果内部网络路由器数量较多时，采用手工配置静态默认路由，则会显得非常繁锁**。因此，建议采用默认网络命令，让 R2 路由器自动的向内部通告默认路由。

9、将 R1 和 R5 的静态默认路由删除后，查看 R1 和 R5 的路由表。如下所示：

```
R1(config)#no ip route 0.0.0.0 0.0.0.0 172.16.1.2
R1(config)#exit
R1#
```

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.1.4 [90/284160] via 172.16.1.2, 00:19:02, FastEthernet0/1
C       172.16.1.0 is directly connected, FastEthernet0/1
R1#
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

```
R5(config)#no ip route 0.0.0.0 0.0.0.0 172.16.1.5
R5(config)#exit
R5#
R5#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.4 is directly connected, Ethernet1/1
D       172.16.1.0 [90/307200] via 172.16.1.5, 00:19:42, Ethernet1/1
R5#
R5#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R5#
```

10、在 R2 上配置默认网络，配置如下所示：

```
R2(config)#router eigrp 50
R2(config-router)#network 192.168.10.0
R2(config-router)#exit
R2(config)#ip default-network 192.168.10.0
R2(config)#exit
R2#show ip route
```

```
Gateway of last resort is 192.168.10.2 to network 0.0.0.0

 *   192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
D*      192.168.10.0/24 is a summary, 00:00:53, Null0
C       192.168.10.0/30 is directly connected, Ethernet1/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.4/30 is directly connected, Ethernet1/2
D       172.16.0.0/16 is a summary, 00:22:22, Null0
C       172.16.1.0/30 is directly connected, Ethernet1/0
S*   0.0.0.0/0 [1/0] via 192.168.10.2
R2#
```

批注 [stanley19]： ip default-network 命令标识的默认网络。

批注 [stanley20]： 手工配置的静态默认路由。

11、查看 R1 和 R5 路由器的路由表，并且尝试访问外部网络：

```
R1#show ip route

Gateway of last resort is 172.16.1.2 to network 192.168.10.0

D*   192.168.10.0/24 [90/284160] via 172.16.1.2, 00:02:03, FastEthernet0/1
     172.16.0.0/30 is subnetted, 2 subnets
D       172.16.1.4 [90/284160] via 172.16.1.2, 00:02:04, FastEthernet0/1
C       172.16.1.0 is directly connected, FastEthernet0/1
R1#
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/105/188 ms
R1#
```

批注 [stanley21]： 由于 R2 上配置的默认网络，EIGRP 路由器会将其通告给 R1 路由器。

```
R5#show ip route

Gateway of last resort is 172.16.1.5 to network 192.168.10.0

D*   192.168.10.0/24 [90/307200] via 172.16.1.5, 00:04:15, Ethernet1/1
     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.4 is directly connected, Ethernet1/1
D       172.16.1.0 [90/307200] via 172.16.1.5, 00:04:19, Ethernet1/1
R5#
R5#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/87/96 ms
R5#
```

12、使用 ip default-network 命令可以有效减少内部网络配置任务。不过需要注意的是 ip default-network 其指出默认网络，建议采用主类网络。如果使用无类网络，则可能会出现无法解释的问题。

38、实验完成。

CCNP Lab Manual

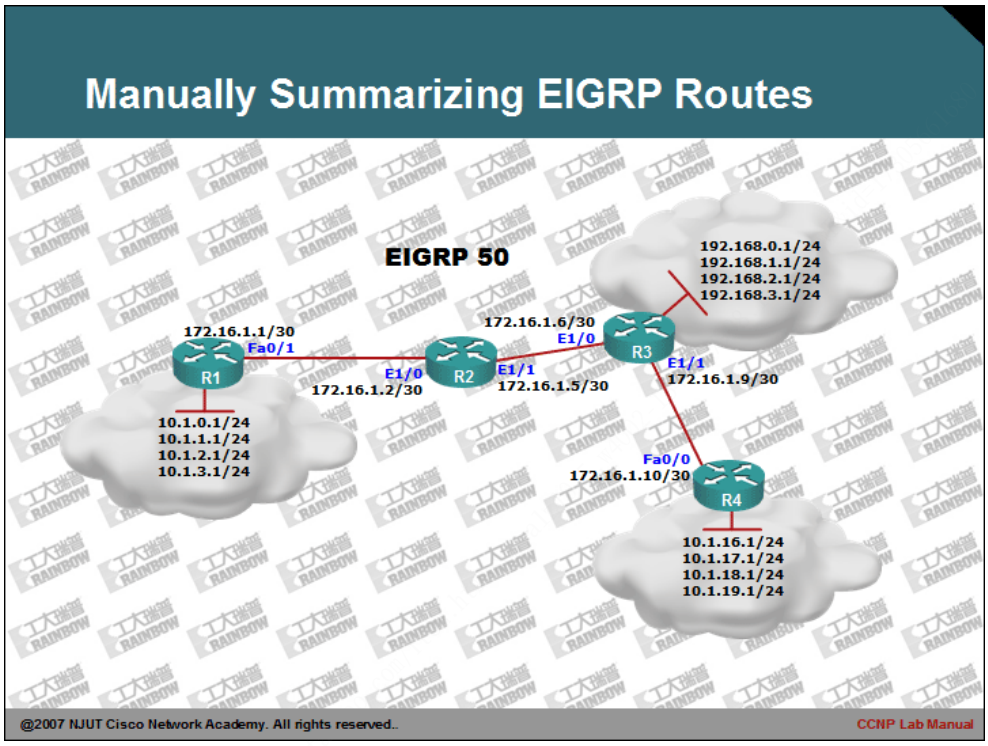
Lab 3. Manually Summarizing EIGRP Routes

实验目的：

1、理解 EIGRP 的自动汇总的缺点。

2、掌握 EIGRP 的手工自动总结的配置方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置各台路由器的 EIGRP 协议,并且不关闭自动总结。

3、在 R2 上使用 ping 测试网络路由，会发现 **R2 路由器无法 ping 通路由器 R4 所连接的 10.1.X.0/24 网络子网**。如下所示：

```
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/46/92 ms
R2#
R2#ping 10.1.16.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.16.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R2#
R2#ping 10.1.17.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.17.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R2#
```

批注 [stanley22]: 无法 ping 通 10.1.16.1 的 IP 地址。

4、查看 R2 的路由表：

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
D       172.16.1.8 [90/307200] via 172.16.1.6, 00:06:25, Ethernet1/1
C       172.16.1.4 is directly connected, Ethernet1/1
C       172.16.1.0 is directly connected, Ethernet1/0
D    10.0.0.0/8 [90/409600] via 172.16.1.1, 00:06:09, Ethernet1/0
D    192.168.0.0/24 [90/409600] via 172.16.1.6, 00:06:25, Ethernet1/1
D    192.168.1.0/24 [90/409600] via 172.16.1.6, 00:06:25, Ethernet1/1
D    192.168.2.0/24 [90/409600] via 172.16.1.6, 00:06:25, Ethernet1/1
```

批注 [stanley23]: R2 路由器显示的汇总路由。

```
D    192.168.3.0/24 [90/409600] via 172.16.1.6, 00:06:25, Ethernet1/1
R2#
```

5、查看 R2 路由器的拓扑数据库：

```
R2#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(50)/ID(172.16.1.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.0.0.0/8, 1 successors, FD is 409600, serno 3
         via 172.16.1.1 (409600/128256), Ethernet1/0
         via 172.16.1.6 (435200/409600), Ethernet1/1
P 192.168.0.0/24, 1 successors, FD is 409600, serno 4
         via 172.16.1.6 (409600/128256), Ethernet1/1
P 192.168.1.0/24, 1 successors, FD is 409600, serno 5
         via 172.16.1.6 (409600/128256), Ethernet1/1
P 192.168.2.0/24, 1 successors, FD is 409600, serno 6
         via 172.16.1.6 (409600/128256), Ethernet1/1
P 192.168.3.0/24, 1 successors, FD is 409600, serno 7
         via 172.16.1.6 (409600/128256), Ethernet1/1
P 172.16.1.8/30, 1 successors, FD is 307200, serno 8
         via 172.16.1.6 (307200/281600), Ethernet1/1
P 172.16.1.4/30, 1 successors, FD is 281600, serno 2
         via Connected, Ethernet1/1
P 172.16.1.0/30, 1 successors, FD is 281600, serno 1
         via Connected, Ethernet1/0
R2#
```

批注 [stanley24]: all-links 参数是显示所有链路。

批注 [stanley25]: 到底 10.0.0.0/8 网络有两条路由。
注意两条路由的FD值是不同的。

6、导致 R2 无法 ping 路由器 R4 所连接的 10.1.X.0/24 的网络主要原因是：R1 本身属于主类的边界，其会将本地路由表中的子网向主类网络自动汇总。而 R4 也属于主类的界，也会与 R1 做出相同的动作。因此 R2 会从不同的接口，收到相同的汇总路由，即 10.0.0.0/8 网络路由。由于 R2 在比较了两条路由的可行距离后，选择了较小的 FD 值的路由，即 R1 通告的 10.0.0.0/8 汇总路由。而忽略了另外一个接口收到汇总路由。其实真正的原因，并不是路由选择出错，而是自动汇总不能做到精确的控制原因导致的。

7、为了解决汇总问题，需要在 R1 和 R4 上关闭自动汇总，而采用手工汇总。配置如下：

```
R1(config)#router eigrp 50
R1(config-router)#no auto-summary
```

批注 [stanley26]: 关闭自动汇总。

```
R1(config-router)#exit
R1(config)#
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip summary-address eigrp 50 10.1.0.0 255.255.252.0
R1(config-if)#exit
R1(config)#exit
```

批注 [stanley27]：进行手工汇总，其汇总路由为 10.1.0.0/22

```
R4(config)#router eigrp 50
R4(config-router)#no auto-summary
R4(config-router)#exit
R4(config)#
R4(config)#interface fastEthernet 0/0
R4(config-if)#ip summary-address eigrp 50 10.1.16.0 255.255.252.0
R4(config-if)#exit
R4(config)#exit
```

8、再次查看 R2 路由表：

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
D       172.16.1.8 [90/307200] via 172.16.1.6, 00:21:08, Ethernet1/1
C       172.16.1.4 is directly connected, Ethernet1/1
C       172.16.1.0 is directly connected, Ethernet1/0
     10.0.0.0/22 is subnetted, 2 subnets
D       10.1.0.0 [90/409600] via 172.16.1.1, 00:03:13, Ethernet1/0
D       10.1.16.0 [90/435200] via 172.16.1.6, 00:01:02, Ethernet1/1
D    192.168.0.0/24 [90/409600] via 172.16.1.6, 00:21:08, Ethernet1/1
D    192.168.1.0/24 [90/409600] via 172.16.1.6, 00:21:08, Ethernet1/1
D    192.168.2.0/24 [90/409600] via 172.16.1.6, 00:21:08, Ethernet1/1
D    192.168.3.0/24 [90/409600] via 172.16.1.6, 00:21:08, Ethernet1/1
R2#
```

批注 [stanley28]：被汇总的/22 位网络路由。

9、再次使用 ping 命令确认网络可达性：

```
R2#ping 10.1.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/69/145 ms
R2#ping 10.1.1.1

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/44/64 ms
R2#ping 10.1.16.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.16.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/97/140 ms
R2#ping 10.1.17.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.17.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/93/149 ms
R2#
```

10、再次查看 R2 的路由表：

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
D       172.16.1.8 [90/307200] via 172.16.1.6, 00:23:45, Ethernet1/1
C       172.16.1.4 is directly connected, Ethernet1/1
C       172.16.1.0 is directly connected, Ethernet1/0
     10.0.0.0/22 is subnetted, 2 subnets
D       10.1.0.0 [90/409600] via 172.16.1.1, 00:05:49, Ethernet1/0
D       10.1.16.0 [90/435200] via 172.16.1.6, 00:03:38, Ethernet1/1
D    192.168.0.0/24 [90/409600] via 172.16.1.6, 00:23:45, Ethernet1/1
D    192.168.1.0/24 [90/409600] via 172.16.1.6, 00:23:45, Ethernet1/1
D    192.168.2.0/24 [90/409600] via 172.16.1.6, 00:23:45, Ethernet1/1
D    192.168.3.0/24 [90/409600] via 172.16.1.6, 00:23:45, Ethernet1/1
R2#
```

批注 [stanley29]: 192.168.X.0/24 具体路由。

11、为了能够有效的减少路由表的大小，还可以通过 EIGRP 对 192.168.X.0/24 的 C 类网络路由进行手工路由汇总，具体配置如下：

```
R3(config)#router eigrp 50
R3(config-router)#no auto-summary
R3(config-router)#exit
R3(config)#
R3(config)#interface ethernet 1/1
R3(config-if)#ip summary-address eigrp 50 192.168.0.0 255.255.252.0
R3(config-if)#exit
```

批注 [stanley30]: 虽然在 R3 上配置的是超网汇总，仍然需要在 R3 的 EIGRP 进程中关闭自动汇总特性，否则，EIGRP 还是会向外通告具体路由。

```
R3(config)#
R3(config)#inter ethernet 1/0
R3(config-if)#ip summary-address eigrp 50 192.168.0.0 255.255.252.0
R3(config-if)#exit
R3(config)#
```

12、查看 R4 和 R2 的路由表：

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.1.8 is directly connected, FastEthernet0/0
D       172.16.1.4 [90/284160] via 172.16.1.9, 00:02:41, FastEthernet0/0
D       172.16.1.0 [90/309760] via 172.16.1.9, 00:02:23, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D       10.1.0.0/22 [90/437760] via 172.16.1.9, 00:02:23, FastEthernet0/0
C       10.1.19.0/24 is directly connected, Loopback0
C       10.1.18.0/24 is directly connected, Loopback0
C       10.1.17.0/24 is directly connected, Loopback0
D       10.1.16.0/22 is a summary, 00:03:33, Null0
C       10.1.16.0/24 is directly connected, Loopback0
D    192.168.0.0/22 [90/156160] via 172.16.1.9, 00:02:41, FastEthernet0/0
R4#
```

批注 [stanley31]: 从R3收到的手工汇总的路由。

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
D       172.16.1.8 [90/307200] via 172.16.1.6, 00:02:54, Ethernet1/1
C       172.16.1.4 is directly connected, Ethernet1/1
C       172.16.1.0 is directly connected, Ethernet1/0
     10.0.0.0/22 is subnetted, 2 subnets
D       10.1.0.0 [90/409600] via 172.16.1.1, 00:16:13, Ethernet1/0
D       10.1.16.0 [90/435200] via 172.16.1.6, 00:02:54, Ethernet1/1
D    192.168.0.0/22 [90/409600] via 172.16.1.6, 00:02:54, Ethernet1/1
R2#
```

批注 [stanley32]: 从R3收到的手工汇总的路由。

13、使用 ping 命令确认路由有效性：

```
R2#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/28/60 ms
R2#
```

```
R4#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/37/48 ms
R4#
```

14、通过本实验可以看出，虽然 EIGRP 的自动汇总能够为网络配置带来便捷，但是其依赖于 IP 子网的规划。如果遇到糟糕的子网规划，则需要小心使用自动特性。

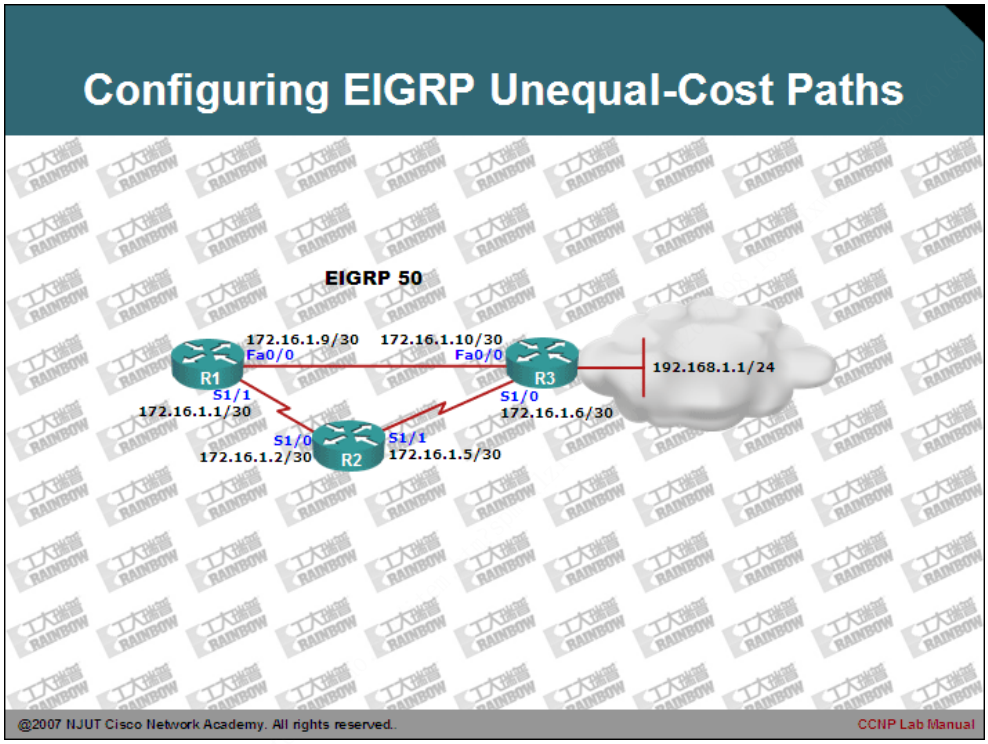
38、实验完成。

Lab 4. Configuring EIGRP Unequal-Cost Paths

实验目的：

1、掌握 EIGRP 的不等价均衡的条件。
2、掌握 EIGRP 的 metric 值修改方法。
3、掌握 EIGRP 的 AD、FD、FC、Successor、FS 概念。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、在三台路由配置 EIGRP 自治系统编号为 50。

3、观察 R1 到达 R3 的 192.168.1.0/24 网络的路由。

```
R1#show ip route

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.1.8 is directly connected, FastEthernet0/0
D       172.16.1.4 [90/2172416] via 172.16.1.10, 00:00:11, FastEthernet0/0
C       172.16.1.0 is directly connected, Serial1/1
D    192.168.1.0/24 [90/156160] via 172.16.1.10, 00:00:11, FastEthernet0/0
R1#
```

批注 [stanley33]：到达 192.168.1.0 的网络的下一跳为 172.16.1.10

4、为了提高网络传输性能，需要同时使用下一跳为 172.16.1.2 的路由，即使用另外一条 metric 值不相等的路径做均衡负载。

5、如果需要使用另外一条路径，则需要确保 R2 成为 R1 到达 192.168.1.0/24 网络的可行后继(FS)，要想成为 FS，则需要满足可行条件(FC)。

6、在 R1 上查看 EIGRP 的拓扑表，没有发现 R2 出现在 R1 的拓扑表中。

```
R1#show ip eigrp 50 topology
.....
P 192.168.1.0/24, 1 successors, FD is 156160
        via 172.16.1.10 (156160/128256), FastEthernet0/0
P 172.16.1.8/30, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
.....
```

批注 [stanley34]：此处，没有出现 R2 的 ip，说明 R2 不是 R1 到达 192.168.1.0/24 的可行后继。

7、查看完整的拓扑表内容。

```
R1#show ip eigrp 50 topology all-links
.....
P 192.168.1.0/24, 1 successors, FD is 156160, serno 6
        via 172.16.1.10 (156160/128256), FastEthernet0/0
        via 172.16.1.2 (2809856/2297856), Serial1/1
.....
```

批注 [stanley35]：通过第 6 步，可以判断 R2 不满足可行条件。

8、确认 FC(可行条件)公式：

AD of secondary-best route < FD of best route(Successor) = Feasible Successor

根据本例可得出：

R2 到达 **192.168.1.0** 网络的 **Distance < 156160**

9、配置 R2 的 EIGRP 的度量，确保 R2 成为 R1 的可行后继者。

```
R2#configure terminal
R2(config)#interface serial 1/1
R2(config-if)#bandwidth 10000000
R2(config-if)#delay 10
R2(config)#exit
```

批注 [stanley36]：通过修改 R2 到达 R3 的串口的带宽和延迟，确保 R2 到达 192.168.1.0/24 的网络的 FD 变小。
此值在 r1 上显示为 AD。

10、查看 R1 的拓扑表。

```
R1#show ip eigrp topology all-links
.....
P 192.168.1.0/24, 1 successors, FD is 156160, serno 6
        via 172.16.1.10 (156160/128256), FastEthernet0/0
        via 172.16.1.2 (2300416/130816), Serial1/1
.....
```

批注 [stanley37]：此时，R1 已经把 R2 当成是自己的可行后继。

11、根据如下公式配置 R1 的 EIGRP 的 variance 值。

FD of FS route < FD of best route(Successor) * Varince

根据公式可得出：

2300416 < 156160 * x

x≈14.73

12、为了测试，先在 R1 上配置 variance 值为 14，观察路由表。

```
R1(config)#router eigrp 50
R1(config-router)#variance 14
R1(config-router)#exit
R1(config)#exit
R1#clear ip router *
R1#show ip route
.....
C       172.16.1.0 is directly connected, Serial1/1
D    192.168.1.0/24 [90/156160] via 172.16.1.10, 00:00:00, FastEthernet0/0
.....
R1#
```

批注 [stanley38]：设置为 14 时，不能满足不等价的条件。

13、将 R1 的 variance 值修改为 15 后，观察路由表。

```
R1(config)#router eigrp 50
R1(config-router)#variance 15
R1(config-router)#exit
R1(config)#exit
R1#clear ip router *
R1#show ip route
.....
C       172.16.1.0 is directly connected, Serial1/1
```

```
D    192.168.1.0/24 [90/156160] via 172.16.1.10, 00:00:01, FastEthernet0/0
                    [90/2300416] via 172.16.1.2, 00:00:01, Serial1/1
R1#
```

批注 [stanley39]: 设置正确的 variance 值后，此处显示为正确的不等价均衡负载的路由。

14、实验完成。

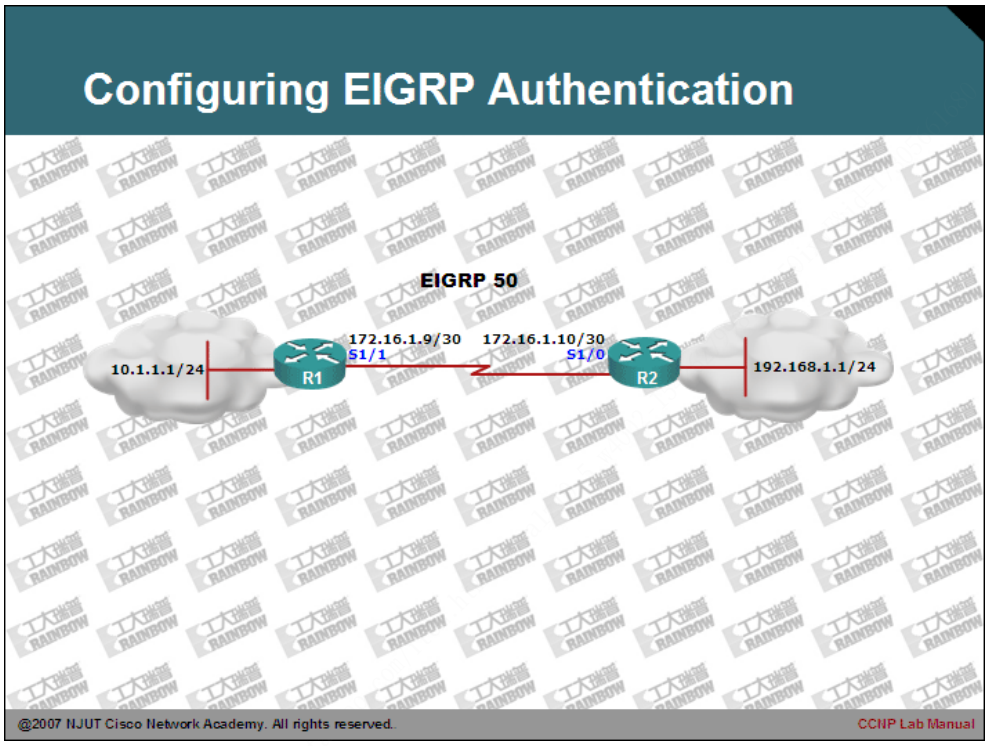
Lab 5. Configuring EIGRP Authentication

实验目的：

1、理解 EIGRP 的认证过程。

2、掌握 EIGRP 的认证的配置。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、在二台路由配置 EIGRP 自治系统编号为 50。

3、查看 R1 与 R2 的路由表。

```
R1#show ip route
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.8/30 is directly connected, Serial1/1
D       172.16.0.0/16 is a summary, 00:00:37, Null0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Loopback0
D       10.0.0.0/8 is a summary, 00:00:37, Null0
D    192.168.1.0/24 [90/2297856] via 172.16.1.10, 00:00:09, Serial1/1
R1#
```

批注 [stanley40]: 从R2学习到的路由

```
R2#show ip route
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.8/30 is directly connected, Serial1/0
D       172.16.0.0/16 is a summary, 00:00:53, Null0
D    10.0.0.0/8 [90/2297856] via 172.16.1.9, 00:00:51, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
R2#
```

4、配置 R1 的 EIGRP 认证。

```
R1#configure terminal
R1(config)#key chain edurainbow
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#
R1(config)#interface serial 1/1
R1(config-if)#ip authentication key-chain eigrp 50 edurainbow
R1(config-if)#ip authentication mode eigrp 50 md5
R1(config-if)#end
R1(config)#
```

批注 [stanley41]: 创建名称为edurainbow的密钥钥匙链

批注 [stanley42]: 创建密码钥匙 1

批注 [stanley43]: 配置密文为 cisco

批注 [stanley44]: 在 s1/1 接口下为 EIGRP 50 启用路由认证。使用 edurainbow 钥匙链。

批注 [stanley45]: 设置认证模式为 md5 加密方式。即密码在传输过程被加密。如果不使用此命令，则密码会以明文方式进行传输。

5、双方路由器使用 clear ip route *命令进行刷新路由表，加快路由表的收敛。

6、查看 R1 与 R2 路由表，观察变化。

```
R1#show ip route
C       172.16.1.8/30 is directly connected, Serial1/1
```

```
D       172.16.0.0/16 is a summary, 00:00:16, Null0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Loopback0
D       10.0.0.0/8 is a summary, 00:00:16, Null0
R1#
```

```
R2#show ip route
.....
C       172.16.1.8/30 is directly connected, Serial1/0
D       172.16.0.0/16 is a summary, 00:02:53, Null0
C    192.168.1.0/24 is directly connected, Loopback0
R2#
```

此时 R1 和 R2 已经无法学习到对方路由器的路由.同时也注意到 R2 路由器系统的反馈信息:

```
*Mar 14 15:35:27.343: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 50: Neighbor 172.16.1.9 (Serial1/0) is
up: new adjacency
*Mar 14 15:35:29.767: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 50: Neighbor 172.16.1.9 (Serial1/0) is
down: Auth failure
```

批注 [stanley46]: R2 路由提示邻居认证失败。

7 查看 R2 的路由表，由于认证失败，此时 R1 与 R2 的邻居关系也无法维持。

```
R2#show ip eigrp 50 neighbors
IP-EIGRP neighbors for process 50


R2#
```

8、配置 R2 的 EIGRP 认证。

```
R2#
R2#configure terminal
R2(config)#key chain edurainbow
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
R2(config-keychain-key)#exit
R2(config-keychain)#exit
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ip authentication key-chain eigrp 50 edurainbow
R2(config-if)#ip authentication mode eigrp 50 md5
R2(config-if)#exit
R2(config)#exit
R2(config)#
```

9、当我们在 R2 路由器上完成认证的配置后，会注意到系统的提示信息：

```
*Mar 14 15:46:04.071: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 50: Neighbor 172.16.1.9 (Serial1/0) is
```

```
up: new adjacency
```

批注 [stanley47]: 新的邻居关系被重新的建立。

同时，查看 R2 的邻居表，会发现 R1 已经成为 R2 的邻居。

```
R2#show ip eigrp 50 neighbors
IP-EIGRP neighbors for process 50
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   172.16.1.9              Se1/0            11 00:01:17   28    200  0  8
R2#
```

批注 [stanley48]: R1 已经成为 R2 的邻居

10、再次使用刷新路由表后，观察 R1 与 R2 的路由表变化。

```
R1#show ip route
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.8/30 is directly connected, Serial1/1
D       172.16.0.0/16 is a summary, 00:08:41, Null0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Loopback0
D       10.0.0.0/8 is a summary, 00:08:42, Null0
D    192.168.1.0/24 [90/2297856] via 172.16.1.10, 00:02:54, Serial1/1
R1#
```

批注 [stanley49]: R1 重新发现了 R2 的路由。

```
R2#show ip route
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.8/30 is directly connected, Serial1/0
D       172.16.0.0/16 is a summary, 00:08:28, Null0
D    10.0.0.0/8 [90/2297856] via 172.16.1.9, 00:03:44, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
R2#
```

批注 [stanley50]: R2 学习到 R1 的路由。

10、实验完成。

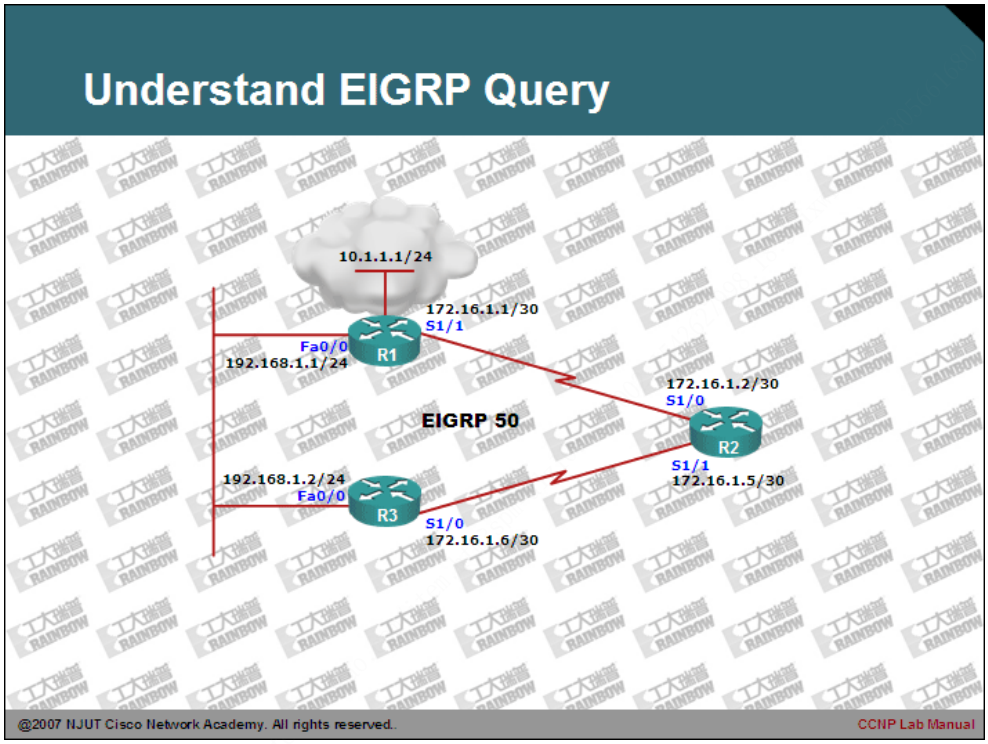
CCNP Lab Manual

Lab 6. Understand EIGRP Query

实验目的：

1、理解 EIGRP 的路由更新机制。
2、掌握 EIGRP 的调试命令。
3、掌握 stub 的配置及使用路由汇总限制 EIGRP 的查询范围。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、在三台路由配置 EIGRP 自治系统编号为 50。**本次实验采用通配符掩码配置 R1 的回环口**。

3、查看 R1、R2 与 R3 确认 EIGRP 工作正常。

```
R1#show ip route eigrp
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.1.4/30 [90/2681856] via 172.16.1.2, 00:01:20, Serial1/1
D       172.16.0.0/16 is a summary, 00:01:00, Null0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:00:59, Null0
R1#
```

```
R2#show ip route eigrp
D    10.0.0.0/8 [90/2297856] via 172.16.1.1, 00:01:16, Serial1/0
D    192.168.1.0/24 [90/2172416] via 172.16.1.1, 00:01:21, Serial1/0
                    [90/2172416] via 172.16.1.6, 00:01:21, Serial1/1
R2#
```

```
R3#sh ip route eigrp
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:01:30, Null0
D       172.16.1.0/30 [90/2681856] via 172.16.1.5, 00:01:36, Serial1/0
D    10.0.0.0/8 [90/156160] via 192.168.1.1, 00:01:30, FastEthernet0/0
R3#
```

4、登录到 R2 路由器，使用 debug 命令跟踪 EIGRP 的更新。

```
R2#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
R2#debug eigrp packets query
EIGRP Packets debugging is on
    (QUERY)
```

批注 [stanley51]：调试 eigrp 的 dual 算法

批注 [stanley52]：调试 eigrp 的查询包

5、在 R1 路由器上使用 shutdown 命令，重激活 loopback 的接口，模拟网络出错。

```
R1(config)#interface loopback 0
R1(config-if)#shutdown
```

6、观察 R2 路由器的调试反馈。

```
*Mar 15 22:03:26.087: EIGRP: Received QUERY on Serial1/0 nbr 172.16.1.1
*Mar 15 22:03:26.091:    AS 50, Flags 0x0, Seq 127/192 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/0
```

批注 [stanley53]：R1 查询 10.1.1.0/24 的网络路由

```
*Mar 15 22:03:26.095: DUAL: rcvquery: 10.1.1.0/24 via 172.16.1.1 metric 4294967295/4294967295,
RD is 2297856
*Mar 15 22:03:26.095: DUAL: Find FS for dest 10.1.1.0/24. FD is 2297856, RD is 2297856
*Mar 15 22:03:26.099: DUAL:     172.16.1.1 metric 4294967295/4294967295
*Mar 15 22:03:26.099: DUAL:     172.16.1.6 metric 2300416/156160 found Dmin is 2300416
*Mar 15 22:03:26.099: DUAL: send REPLY(R1/n1) about 10.1.1.0/24 to 172.16.1.1
*Mar 15 22:03:26.099: DUAL: RT installed 10.1.1.0/24 via 172.16.1.6
*Mar 15 22:03:26.099: DUAL: Send update about 10.1.1.0/24.  Reason: metric chg
*Mar 15 22:03:26.099: DUAL: Send update about 10.1.1.0/24.  Reason: new if
*Mar 15 22:03:26.147: EIGRP: Received QUERY on Serial1/1 nbr 172.16.1.6
*Mar 15 22:03:26.151:   AS 50, Flags 0x0, Seq 144/194 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/0
*Mar 15 22:03:26.155: DUAL: rcvquery: 10.1.1.0/24 via 172.16.1.6 metric 4294967295/4294967295,
RD is 2300416
*Mar 15 22:03:26.155: DUAL: Find FS for dest 10.1.1.0/24. FD is 2297856, RD is 2300416
*Mar 15 22:03:26.159: DUAL:     172.16.1.6 metric 4294967295/4294967295
*Mar 15 22:03:26.159: DUAL:     172.16.1.1 metric 4294967295/4294967295 not found Dmin is
4294967295
*Mar 15 22:03:26.159: DUAL: Peer total/stub 2/0 template/full-stub 2/0
*Mar 15 22:03:26.159: DUAL: Dest 10.1.1.0/24 entering active state.
*Mar 15 22:03:26.159: DUAL: Set reply-status table. Count is 2.
*Mar 15 22:03:26.159: DUAL: Not doing split horizon
*Mar 15 22:03:26.159: DUAL: Going from state 1 to state 3
*Mar 15 22:03:26.171: EIGRP: Enqueueing QUERY on Serial1/1 iidbQ un/rely 0/1 serno 148-148
*Mar 15 22:03:26.175: EIGRP: Enqueueing QUERY on Serial1/1 nbr 172.16.1.6 iidbQ un/rely 0/0
peerQ un/rely 0/0 serno 148-148
*Mar 15 22:03:26.179: EIGRP: Sending QUERY on Serial1/1 nbr 172.16.1.6
*Mar 15 22:03:26.179:   AS 50, Flags 0x0, Seq 195/144 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/1 serno 148-148
*Mar 15 22:03:26.199: EIGRP: Enqueueing QUERY on Serial1/0 iidbQ un/rely 0/1 serno 148-148
*Mar 15 22:03:26.203: EIGRP: Enqueueing QUERY on Serial1/0 nbr 172.16.1.1 iidbQ un/rely 0/0
peerQ un/rely 0/0 serno 148-148
*Mar 15 22:03:26.207: EIGRP: Sending QUERY on Serial1/0 nbr 172.16.1.1
*Mar 15 22:03:26.207:   AS 50, Flags 0x0, Seq 196/127 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/1 serno 148-148
*Mar 15 22:03:26.215: DUAL: rcvreply: 10.1.1.0/24 via 172.16.1.6 metric 4294967295/4294967295
*Mar 15 22:03:26.219: DUAL: reply count is 2
*Mar 15 22:03:26.219: DUAL: Clearing handle 1, count now 1
*Mar 15 22:03:26.267: DUAL: rcvreply: 10.1.1.0/24 via 172.16.1.1 metric 4294967295/4294967295
*Mar 15 22:03:26.267: DUAL: reply count is 1
*Mar 15 22:03:26.267: DUAL: Clearing handle 0, count now 0
*Mar 15 22:03:26.271: DUAL: Freeing reply status table
*Mar 15 22:03:26.271: DUAL: Find FS for dest 10.1.1.0/24. FD is 4294967295, RD is 4294967295
```

批注 [stanley54]： 发现 fs，直接回复 R1。R2 使用 172.16.1.6 作为下一跳到达 10.1.1.0/24 的网络。**其主要是因为时间差的原因造成的。其实 R3 此时也无法到达 10.1.1.0/24 的网络。**

批注 [stanley55]： 安装 172.16.1.6 的下一跳路由到路由表。

批注 [stanley56]： 随后收到 R3 路由查询 10.1.1.0/24 网络路由。

批注 [stanley57]： 无法找到到达 10.1.1.0/24 的 fs。

批注 [stanley58]： 向 R3 发起查询 10.1.1.0/24 网络路由

批注 [stanley59]： 向 R1 发起查询 10.1.1.0/24 网络路由

```
found
.........
```

根据提示，可以发现共有 4 查询包，与之相对应的会产生 4 个回复包。如果在实际应用中，使用 EIGRP 的网络可以多达数十台及数百台路由，那么如果出现某个网络出错，则有可以引起整个网络产生大量的查询回复包。所以为了避免这样的问题，可以使用 ip summary 命令或 stub 参数来进行配置 EIGRP，限制 EIGRP 的查询范围。

7、登录到 R1 和 R3 路由器上配置汇总。

```
R1(config)#interface loopback 0
R1(config-if)#no shutdown
R1(config)#interface serial 1/1
R1(config-if)#ip summary-address eigrp 50 10.0.0.0 255.0.0.0
```

批注 [stanley60]: 激活 loopback0 的接口

批注 [stanley61]: 进行子网汇总。

```
R3(config)#interface serial 1/0
R3(config-if)#ip summary-address eigrp 50 10.0.0.0 255.0.0.0
```

批注 [stanley62]: 进行子网汇总。

8、再次观察 R2 与 R3 的路由表，确认已经学习到 10.1.1.0/24 的网络汇总路由。

```
R2#show ip route eigrp
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.0.0/16 [90/2684416] via 172.16.1.1, 00:15:27, Serial1/0
     10.0.0.0/24 is subnetted, 1 subnets
D       10.1.1.0 [90/2297856] via 172.16.1.1, 00:00:27, Serial1/0
D    192.168.1.0/24 [90/2172416] via 172.16.1.1, 00:15:09, Serial1/0
                    [90/2172416] via 172.16.1.6, 00:15:09, Serial1/1
R2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/78/104 ms
R2#
```

```
R3>show ip route eigrp

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:15:43, Null0
D       172.16.1.0/30 [90/2172416] via 192.168.1.1, 00:15:43, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
D       10.1.1.0 [90/156160] via 192.168.1.1, 00:00:57, FastEthernet0/0
R3>
R3>ping 10.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/62/96 ms
R3>
```

9、在 R1 路由器上，再次 shutdown 掉 loopback0 接口，同时观察 R2 的 debug 信息。

```
*Mar 15 22:11:17.867: EIGRP: Received QUERY on Serial1/0 nbr 172.16.1.1
*Mar 15 22:11:17.871:   AS 50, Flags 0x0, Seq 135/207 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/0
*Mar 15 22:11:17.875: DUAL: dest(10.1.1.0/24) not active
*Mar 15 22:11:17.875: DUAL: rcvquery: 10.1.1.0/24 via 172.16.1.1 metric 4294967295/4294967295,
RD is 4294967295
*Mar 15 22:11:17.879: DUAL: send REPLY(R1/n1) about 10.1.1.0/24 to 172.16.1.1
*Mar 15 22:11:17.879: DUAL: rcvquery: 10.0.0.0/8 via 172.16.1.1 metric 4294967295/4294967295,
RD is 2297856
*Mar 15 22:11:17.883: DUAL: Find FS for dest 10.0.0.0/8. FD is 2297856, RD is 2297856
*Mar 15 22:11:17.883: DUAL:     172.16.1.1 metric 4294967295/4294967295
*Mar 15 22:11:17.887: DUAL:     172.16.1.6 metric 2300416/156160 found Dmin is 2300416
*Mar 15 22:11:17.887: DUAL: send REPLY(R1/n1) about 10.0.0.0/8 to 172.16.1.1
*Mar 15 22:11:17.891: DUAL: RT installed 10.0.0.0/8 via 172.16.1.6
*Mar 15 22:11:17.895: DUAL: Send update about 10.0.0.0/8.  Reason: metric chg
*Mar 15 22:11:17.895: DUAL: Send update about 10.0.0.0/8.  Reason: new if
*Mar 15 22:11:17.899: EIGRP: Received QUERY on Serial1/1 nbr 172.16.1.6
*Mar 15 22:11:17.903:   AS 50, Flags 0x0, Seq 154/208 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/0
*Mar 15 22:11:17.907: DUAL: dest(10.1.1.0/24) not active
*Mar 15 22:11:17.907: DUAL: rcvquery: 10.1.1.0/24 via 172.16.1.6 metric 4294967295/4294967295,
RD is 4294967295
*Mar 15 22:11:17.911: DUAL: send REPLY(R1/n1) about 10.1.1.0/24 to 172.16.1.6
*Mar 15 22:11:17.951: DUAL: Removing dest 10.1.1.0/24, nexthop 172.16.1.1
*Mar 15 22:11:17.955: DUAL: Removing dest 10.0.0.0/8, nexthop 172.16.1.1
*Mar 15 22:11:18.015: DUAL: Removing dest 10.1.1.0/24, nexthop 172.16.1.6
*Mar 15 22:11:18.015: DUAL: No routes.  Flushing dest 10.1.1.0/24
*Mar 15 22:11:18.019: EIGRP: Received QUERY on Serial1/1 nbr 172.16.1.6
*Mar 15 22:11:18.023:   AS 50, Flags 0x0, Seq 157/212 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/0
*Mar 15 22:11:18.027: DUAL: rcvquery: 10.0.0.0/8 via 172.16.1.6 metric 4294967295/4294967295,
RD is 2300416
*Mar 15 22:11:18.027: DUAL: Find FS for dest 10.0.0.0/8. FD is 2297856, RD is 2300416
*Mar 15 22:11:18.031: DUAL:     172.16.1.6 metric 4294967295/4294967295 not found Dmin is
4294967295
```

批注 [stanley63]： R1 查询 10.1.1.0/24 网络路由

批注 [stanley64]： R1 查询 10.0.0.0/8 的网络。**此查询主要是汇总造成的。下面会解释如何避免此查询。**

批注 [stanley65]： R3 查询 10.1.1.0/24 的网络路由

批注 [stanley66]： R3 查询 10.0.0.0/8 的网路路由。**此查询也是由汇总造成的。**

```
*Mar 15 22:11:18.031: DUAL: Peer total/stub 2/0 template/full-stub 2/0
*Mar 15 22:11:18.035: DUAL: Dest 10.0.0.0/8 entering active state.
*Mar 15 22:11:18.035: DUAL: Set reply-status table. Count is 1.
*Mar 15 22:11:18.039: DUAL: Doing split horizon on Serial1/1
*Mar 15 22:11:18.039: DUAL: Going from state 1 to state 3
*Mar 15 22:11:18.047: EIGRP: Enqueueing QUERY on Serial1/1 iidbQ un/rely 0/1 serno 161-161
*Mar 15 22:11:18.051: EIGRP: Enqueueing QUERY on Serial1/0 iidbQ un/rely 0/1 serno 161-161
*Mar 15 22:11:18.051: EIGRP: Enqueueing QUERY on Serial1/1 nbr 172.16.1.6 iidbQ un/rely 0/0
peerQ un/rely 0/0 serno 161-161
*Mar 15 22:11:18.055: EIGRP: Enqueueing QUERY on Serial1/0 nbr 172.16.1.1 iidbQ un/rely 0/0
peerQ un/rely 0/0 serno 161-161
*Mar 15 22:11:18.063: EIGRP: Sending QUERY on Serial1/0 nbr 172.16.1.1
*Mar 15 22:11:18.063:    AS 50, Flags 0x0, Seq 214/135 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/1 serno 161-161
*Mar 15 22:11:18.119: DUAL: dest(10.0.0.0/8) active
*Mar 15 22:11:18.119: DUAL: rcvreply: 10.0.0.0/8 via 172.16.1.1 metric 4294967295/4294967295
*Mar 15 22:11:18.123: DUAL: reply count is 1
*Mar 15 22:11:18.123: DUAL: Clearing handle 0, count now 0
*Mar 15 22:11:18.123: DUAL: Freeing reply status table
*Mar 15 22:11:18.123: DUAL: Find FS for dest 10.0.0.0/8. FD is 4294967295, RD is 4294967295
found
*Mar 15 22:11:18.127: DUAL: send REPLY(R1/n1) about 10.0.0.0/8 to 172.16.1.6
*Mar 15 22:11:18.131: DUAL: Removing dest 10.0.0.0/8, nexthop 172.16.1.1
*Mar 15 22:11:18.131: DUAL: Going from state 3 to state 1
*Mar 15 22:11:18.171: DUAL: Removing dest 10.0.0.0/8, nexthop 172.16.1.6
*Mar 15 22:11:18.171: DUAL: No routes.  Flushing dest 10.0.0.0/8
```

批注 [stanley67]: 向R1查询10.0.0.0/8的路由。

通过配置汇总，我们可以发现，本次查询中只有 2 次关于 10.1.1.0/24 的网络查询。**另外 3 个查询是由于配置了汇总后。R1 和 R3 查询 10.0.0.0/8 的网络而产生的。**

10、为了能够彻底解决查询的问题。我们在 R2 上配置 EIGRP stub 的特性。以阻止向路由器 R2 查询 10.0.0.0/8 的网络路由:

```
R2(config)#router eigrp 50
R2(config-router)#eigrp stub
```

批注 [stanley68]: 配置R2为末节属性。

11、在 R1 或是 R2 的任一路由器上查看邻居表，观察末节特性。

```
R1#show ip eigrp neighbors detail
IP-EIGRP neighbors for process 50
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   172.16.1.2              Se1/1             12 00:01:01  216  1296  0  220
   Version 12.3/1.2, Retrans: 0, Retries: 0
```

```
   Stub Peer Advertising ( CONNECTED SUMMARY ) Routes
   Suppressing queries
1    192.168.1.2             Fa0/0             14 01:09:11    75    450  0   159
   Version 12.3/1.2, Retrans: 1, Retries: 0
R1#
```

批注 [stanley69]: EIGRP 不会向被配置了末节特性的路由器查询其它网络的路由。

12、再次对 R1 的 loopback 0 的接口激活再禁用一次，观察 R2 路由器的提示信息：

```
*Mar 15 22:22:31.371: DUAL: rcvupdate: 10.0.0.0/8 via 172.16.1.1 metric 4294967295/4294967295
*Mar 15 22:22:31.371: DUAL: Find FS for dest 10.0.0.0/8. FD is 2297856, RD is 2297856
*Mar 15 22:22:31.375: DUAL:      172.16.1.1 metric 4294967295/4294967295
*Mar 15 22:22:31.375: DUAL:      172.16.1.6 metric 2300416/156160 found Dmin is 2300416
*Mar 15 22:22:31.379: DUAL: Removing dest 10.0.0.0/8, nexthop 172.16.1.1
*Mar 15 22:22:31.383: DUAL: RT installed 10.0.0.0/8 via 172.16.1.6
*Mar 15 22:22:31.383: DUAL: Send update about 10.0.0.0/8.  Reason: metric chg
*Mar 15 22:22:31.387: DUAL: Send update about 10.0.0.0/8.  Reason: new if
*Mar 15 22:22:31.587: DUAL: rcvupdate: 10.0.0.0/8 via 172.16.1.6 metric 4294967295/4294967295
*Mar 15 22:22:31.587: DUAL: Find FS for dest 10.0.0.0/8. FD is 2297856, RD is 2300416
*Mar 15 22:22:31.591: DUAL:      172.16.1.6 metric 4294967295/4294967295 not found Dmin is
4294967295
*Mar 15 22:22:31.591: DUAL: Peer total/stub 2/0 template/full-stub 2/0
*Mar 15 22:22:31.595: DUAL: Dest 10.0.0.0/8 entering active state.
*Mar 15 22:22:31.595: DUAL: Set reply-status table. Count is 2.
*Mar 15 22:22:31.595: DUAL: Not doing split horizon
*Mar 15 22:22:31.607: EIGRP: Enqueueing QUERY on Serial1/1 iidbQ un/rely 0/1 serno 169-169
*Mar 15 22:22:31.607: EIGRP: Enqueueing QUERY on Serial1/0 iidbQ un/rely 0/1 serno 169-169
*Mar 15 22:22:31.611: EIGRP: Enqueueing QUERY on Serial1/1 nbr 172.16.1.6 iidbQ un/rely 0/0
peerQ un/rely 0/0 serno 169-169
*Mar 15 22:22:31.615: EIGRP: Enqueueing QUERY on Serial1/0 nbr 172.16.1.1 iidbQ un/rely 0/0
peerQ un/rely 0/0 serno 169-169
*Mar 15 22:22:31.619: EIGRP: Sending QUERY on Serial1/1 nbr 172.16.1.6
*Mar 15 22:22:31.623:   AS 50, Flags 0x0, Seq 226/169 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/1 serno 169-169
*Mar 15 22:22:31.627: EIGRP: Sending QUERY on Serial1/0 nbr 172.16.1.1
*Mar 15 22:22:31.627:   AS 50, Flags 0x0, Seq 227/148 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely
0/1 serno 169-169
*Mar 15 22:22:31.711: DUAL: dest(10.0.0.0/8) active
*Mar 15 22:22:31.715: DUAL: rcvreply: 10.0.0.0/8 via 172.16.1.1 metric 4294967295/4294967295
*Mar 15 22:22:31.715: DUAL: reply count is 2
.....
```

批注 [stanley70]: 向 R1 查询 10.0.0.0/8 网络路由

批注 [stanley71]: 向 R2 查询 10.0.0.0/8 网络路由

经过如上配置后，会发现 R2 路由器，不会再接收到任何的关于 10.1.1.0/24 的网络的查询包。仅仅有关于 10.0.0.0/8 网络的本地查询包被发出。因此使用汇

总和 stub 可以有效的避免路由出现 SIA 状态，同时解决了 EIGRP 的路由收敛问题,保证 EIGRP 的收敛变得简单可行。

13、实验完成。

CCNP Lab Manual

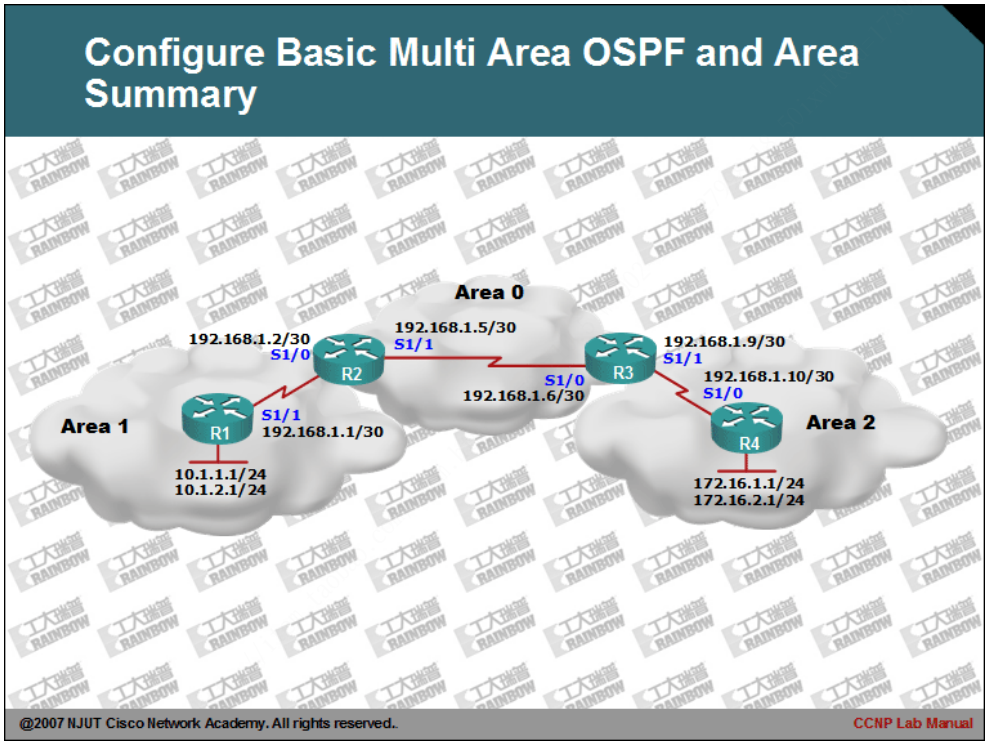
Lab 7. Configuring Basic Multi Area OSPF and Area Summary

Summary

实验目的：

1、掌握多区域的 OSPF 配置方法。
2、区别不同区域的路由。
3、掌握 OSPF 的路由汇总配置。
4、掌握 OSPF 的基本配置命令。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、在 R1 上进行 area 1 区域 OSPF 配置。

```
R1(config)#router ospf 1
R1(config-router)#network 10.1.2.0 0.0.0.255 area 1
R1(config-router)#network 10.1.1.0 0.0.0.255 area 1
R1(config-router)#network 192.168.1.0 0.0.0.3 area 1
R1(config-router)#exit
```

批注 [stanley72]: 在配置 network 时,使用 area 参数指出从属于哪一个区域.

3、在 R2 上进行 area1 与 area2 的区域边界路由器(ABR)的 OSPF 配置。

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.3 area 1
R2(config-router)#network 192.168.1.4 0.0.0.3 area 0
R2(config)#exit
```

批注 [stanley73]: 区域 1 的 network

批注 [stanley74]: 区域 0 的 network

4、参照 R1 与 R2 的配置，完成 R3 与 R4 的配置。

5、在任一路由器上，查看 OSPF 邻居表。

```
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.9       1   FULL/  -        00:00:39    192.168.1.6     Serial1/1
10.1.2.1          1   FULL/  -        00:00:37    192.168.1.1     Serial1/0
R2#
```

批注 [stanley75]: R2 路由器已经成功与 R1 与 R3 建立邻居关系。

6、查看 R1 的路由表，观察其它区域路由。

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

.....
Gateway of last resort is not set
     172.16.0.0/32 is subnetted, 2 subnets
O IA    172.16.1.1 [110/193] via 192.168.1.2, 00:02:23, Serial1/1
O IA    172.16.2.1 [110/193] via 192.168.1.2, 00:02:23, Serial1/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback1
C       10.1.1.0 is directly connected, Loopback0
     192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/192] via 192.168.1.2, 00:02:58, Serial1/1
C       192.168.1.0 is directly connected, Serial1/1
```

批注 [stanley76]: 其它区域的路由会使用 IA 作为前缀。
IA=>OSPF inter area

批注 [stanley77]: OSPF 的管理距离为 110。

```
O IA    192.168.1.4 [110/128] via 192.168.1.2, 00:05:06, Serial1/1
R1#
```

批注 [stanley78]: OSPF 对于此链路计算的 cost 值。**Cost= 10^8 / Bandwidth** 需要注意的是此处 bandwidth 并不是指链路的物理带宽。其可以通过 bandwidth 命令进行修改。Serial 接口默认的带宽为 T1 即 1.544Mbps。

7、查看 R1 的 OSPF 链路状态数据库。

```
R1#show ip ospf database

            OSPF Router with ID (10.1.2.1) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.2.1        10.1.2.1        492         0x80000004 0x00C83F 4
192.168.1.5     192.168.1.5     486         0x80000003 0x002BB5 2

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.1.1      192.168.1.5     315         0x80000001 0x00CCC0
172.16.2.1      192.168.1.5     315         0x80000001 0x00C1CA
192.168.1.4     192.168.1.5     479         0x80000001 0x00E33E
192.168.1.8     192.168.1.5     350         0x80000001 0x003E9F
R1#
```

批注 [stanley79]: 类型 1 的 LSA。

批注 [stanley80]: 类型 3 的 LSA，描述区域间的路由。

8、在 R1 上使用 ping 命令确认路由的有效性。

```
R1#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 216/240/288 ms
R1#
```

9、查看 R4 的路由表和 ospf 的链路状态数据库。

```
R4#show ip route
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback1
     10.0.0.0/24 is subnetted, 2 subnets
O IA    10.1.2.0 [110/193] via 192.168.1.9, 00:15:14, Serial1/0
O IA    10.1.1.0 [110/193] via 192.168.1.9, 00:15:14, Serial1/0
     192.168.1.0/30 is subnetted, 3 subnets
C       192.168.1.8 is directly connected, Serial1/0
O IA    192.168.1.0 [110/192] via 192.168.1.9, 00:15:14, Serial1/0
O IA    192.168.1.4 [110/128] via 192.168.1.9, 00:15:14, Serial1/0
R4#
```

```
R4#show ip ospf database

            OSPF Router with ID (172.16.2.1) (Process ID 1)

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.2.1      172.16.2.1      1223        0x80000004 0x00B871 4
192.168.1.9     192.168.1.9     1224        0x80000002 0x00EA2E 2

                Summary Net Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.1.0        192.168.1.9     2           0x80000001 0x00B586
10.1.2.0        192.168.1.9     2           0x80000001 0x00AA90
192.168.1.0     192.168.1.9     1265        0x80000001 0x00766B
192.168.1.4     192.168.1.9     1265        0x80000001 0x00CB52
R4#
```

批注 [stanley81]: 关于 area 1 的两条类型 3 的 LSA.。

可以发现 R4 路由器学习到 area1 区域的具体路由，其实，可以通过在 R2(ABR)上可以对 area1 的路由进行汇总，通过汇总可以有效的减少路由表的大小，限制 LSA 扩散。

10、配置 R2 的区域汇总。

```
R2(config)#router ospf 1
R2(config-router)#area 1 range 10.1.0.0 255.255.0.0
R2(config-router)#exit
R2(config)#exit
```

批注 [stanley82]: 使用 area 1 range 命令对区域 1 的路由进行汇总。

11、再次查看 R4 的路由表和数据库。

```
R4#show ip route
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback1
     10.0.0.0/16 is subnetted, 1 subnets
O IA    10.1.0.0 [110/193] via 192.168.1.9, 00:00:32, Serial1/0
     192.168.1.0/30 is subnetted, 3 subnets
C       192.168.1.8 is directly connected, Serial1/0
O IA    192.168.1.0 [110/192] via 192.168.1.9, 00:18:36, Serial1/0
O IA    192.168.1.4 [110/128] via 192.168.1.9, 00:18:36, Serial1/0
R4#
R4#show ip ospf database

            OSPF Router with ID (172.16.2.1) (Process ID 1)
```

批注 [stanley83]: Area 1 的路由已经成功的被汇总。如果 area 1 存在多条路由的话，这样做是很有实际意义的。

```
                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.2.1      172.16.2.1      6           0x80000005 0x00B672 4
192.168.1.9     192.168.1.9     13          0x80000004 0x00E630 2

                Summary Net Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum
10.1.0.0        192.168.1.9     29          0x80000001 0x00C07C
192.168.1.0     192.168.1.9     1325        0x80000001 0x00766B
192.168.1.4     192.168.1.9     1325        0x80000001 0x00CB52
R4#
```

批注 [stanley84]: 对于 area 1 的区域仅有一条类型 3 的 LSA。

12、实验完成。

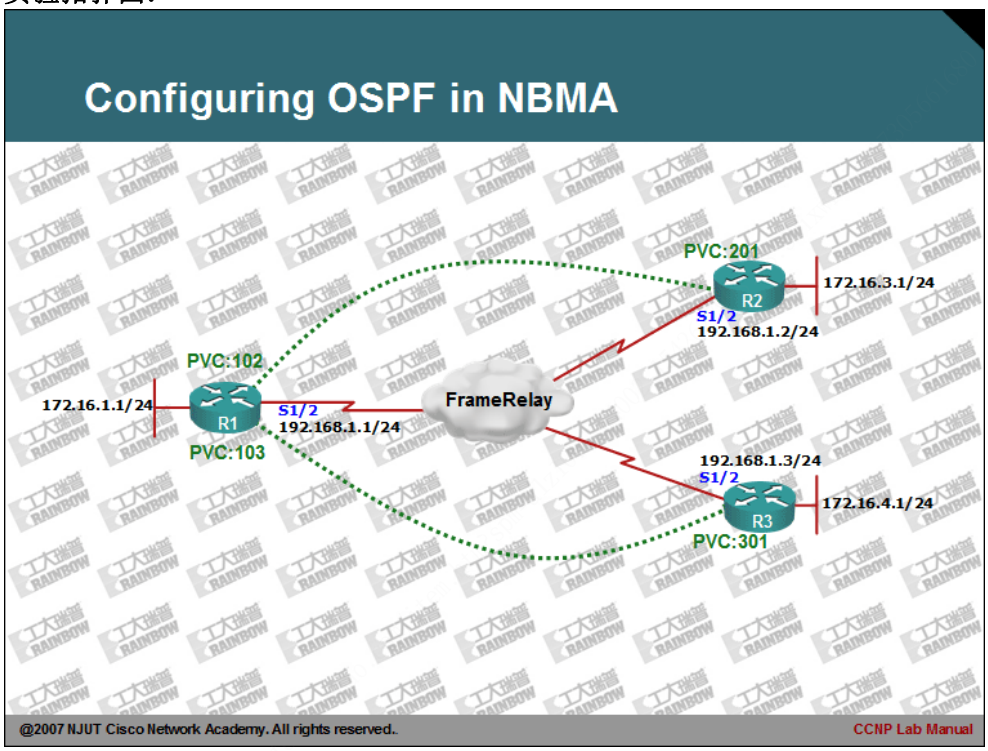
Lab 8. Configuring OSPF in NBMA

实验目的：

1、掌握 NBMA 网络中 OSPF 的邻居关系手工和自动建立的两种配置方法。

2、掌握指定 OSPF 的接口优先级和通过修改 OSPF 的默认接口网络类型避免 DR 的选举出错。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、其中 R1、R2 和 R3 的配置如下：

```
R1(config)#interface loopback 0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip ospf network point-to-point
R1(config-if)#exit
R1(config)#
R1(config)#interface serial 1/2
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no frame-relay inverse-arp
R1(config-if)#frame-relay map ip 192.168.1.2 102 broadcast
R1(config-if)#frame-relay map ip 192.168.1.3 103 broadcast
R1(config-if)#exit
R1(config)#
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.1.0 0.0.0.255 area 0
R1(config-router)#exit
R1(config)#
```

批注 [stanley85]： 避免其环回接口地址被 OSPF 学习为/32 的主机地址。

批注 [stanley86]： 关闭反向 ARP。

批注 [stanley87]： 采用手工映射配置。主要目的是配置星形的帧中继拓扑网络。并且在映射时，采用 BROADCAST 关键字，以便帧中继可以支持广播的转发。

```
R2(config)#interface loopback 0
R2(config-if)#ip address 172.16.3.1 255.255.255.0
R2(config-if)#ip ospf network point-to-point
R2(config-if)#exit
R2(config)#
R2(config)#interface serial 1/2
R2(config-if)#encapsulation frame-relay
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#no frame-relay inverse-arp
R2(config-if)#frame-relay map ip 192.168.1.1 201 broadcast
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#router ospf 1
R2(config-router)#network 172.16.3.0 0.0.0.255 area 0
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#exit
R2(config)#
```

```
R3(config)#interface loopback 0
R3(config-if)#ip address 172.16.4.1 255.255.255.0
R3(config-if)#ip ospf network point-to-point
R3(config-if)#exit
R3(config)#
R3(config)#interface serial 1/2
R3(config-if)#ip address 192.168.1.3 255.255.255.0
R3(config-if)#encapsulation frame-relay
R3(config-if)#no frame-relay inverse-arp
R3(config-if)#frame-relay map ip 192.168.1.1 301 broadcast
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
R3(config)#router ospf 1
R3(config-router)#network 172.16.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.1.0 0.0.0.255 area 0
R3(config-router)#exit
R3(config)#
```

3、在配置完 OSPF 协议后，查看 R1、R2 或 R3 路由器 OSPF 的邻居表，会发现 OSPF 的邻居关系并没有被建立：

```
R1#show ip ospf neighbor


R1#
```

4、查看 R1 的 Seiral 1/2 接口 OSPF 信息：

```
R1#show ip ospf interface serial 1/2
Serial1/2 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 172.16.1.1, Network Type NON_BROADCAST, Cost: 64
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.1.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:15
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R1#
```

批注 [stanley88]： OSPF 默认会把帧中继的接口看成非广播的网络，而不受映射时是否追加 BROADCAST 的参数影响。

5、通过分析可以看出，影响 OSPF 协议不能自己形成邻居关系的主要原因是，OSPF 主观 认为 NBMA 的广播不支持广播和组播，因此不会主动的向外发送 OSPF 的 HELLO 数据包。

6、手工配置 R1 路由器的 OSPF 邻居关系：

```
R1(config)#router ospf 1
R1(config-router)#neighbor 192.168.1.2
R1(config-router)#neighbor 192.168.1.3
```

批注 [stanley89]：手工指定 OSPF 的邻居，当配置完此命令后，OSPF 会采用单播数据包与邻居联系，建立邻居关系。

```
R2(config)#router ospf 1
R2(config-router)#neighbor 192.168.1.1
```

```
R3(config)#router ospf 1
R3(config-router)#neighbor 192.168.1.1
```

7、当配置完成后，系统 IOS 会提示如下信息：

```
*Jun 18 15:36:16.743: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.4.1 on Serial1/2 from LOADING to FULL, Loading Done
*Jun 18 15:36:16.747: %OSPF-5-ADJCHG: Process 1, Nbr 172.16.3.1 on Serial1/2 from LOADING to FULL, Loading Don
```

批注 [stanley90]：邻居关系成功的创建。

8、查看 R1 的邻居表：

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.1        1   FULL/DROTHER    00:01:31    192.168.1.2     Serial1/2
172.16.4.1        1   FULL/DR         00:01:57    192.168.1.3     Serial1/2
R1#
```

9、除了手工的配置方法之外，其实也可能修改 OSPF 的接口类型，以便路由器能够自动的创建 OSPF 的邻居关系，配置比较简单，也不容易出错。首先，将之前配置的 neighbor 的命令给 no 掉。然后再做配置如下：

```
R1(config)#interface serial 1/2
R1(config-if)#ip ospf network broadcast
R1(config-if)#exit
```

批注 [stanley91]：强制配置 S1/2 的接口为广播类型的接口。

10、查看接口信息：

```
R1#show ip ospf interface serial 1/2
Serial1/2 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 172.16.1.1, Network Type BROADCAST, Cost: 64
Transmit Delay is 1 sec, State DR, Priority 1
.....
```

```
R1#
```

11、查看 R1、R2 和 R3 路由器的 OSPF 邻居表：

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.1        1   FULL/DROTHER    00:00:32    192.168.1.2     Serial1/2
172.16.4.1        1   FULL/DR         00:00:33    192.168.1.3     Serial1/2
R1#
```

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/BDR        00:00:30    192.168.1.1     Serial1/2
R2#
```

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/BDR        00:00:39    192.168.1.1     Serial1/2
R3#
```

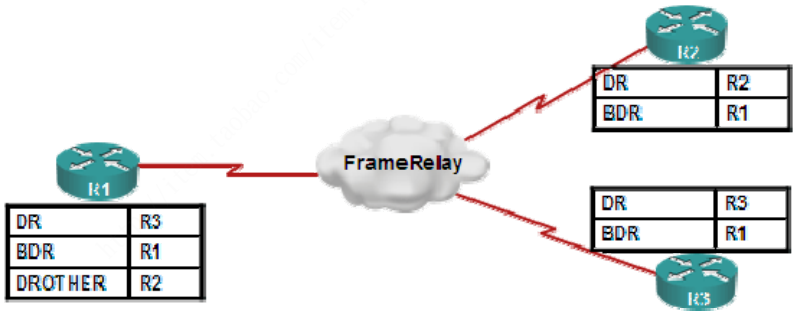
12、仔细观察 OSPF 的邻居表，会发现如下问题：

R1 的 OSPF 邻居表，指出 172.16.4.1 为 DR，172.16.3.1 为 DROTHER，而自己为 BDR。

R2 的 OSPF 邻居表，指出 172.16.1.1 为 BDR，而自己为 DR。

R3 的 OSPF 邻居表，指出 172.16.1.1 为 BDR，而自己为 DR。

通过如下图示，可以更清楚看出 DR 和 BDR 的关系：



出现此问题的原因是因为 Frame-Relay 的网络拓扑非全网状。R3 在与 R1 在进行邻居创建时，R3 并不知道网络中还有 R2 的存在。同时，R2 与 R1 进行创建时，也不知晓 R3 的存在。此时，在网络中运行的其实是两个不同的 OSPF 的自治系统。

13、由于上述的问题，还会导致其它原因，比如：R3 路由器的 172.16.4.0/24 的子网出错，R3 会向 R1 通告 LSA，R1 在收到此 LSA 后，R1 并不会向 R3 转发，其原因是，R1 认为 R3 是由 DR 来完成通告的。其遵守 OSPF 的多路访问网络的更新规则。另外：如果 R1 的 172.16.1.0/24 网络出错，R1 默认会向 DR 通告，即向 R3 通告，而不会向 R2 通告，因为 R1 作为 BDR，只需要将 LSA 通告给 DR 即可，而其它的 DROTHER 的通告是由 DR 完成的，而做为 DR 的 R3 在收到 R1 发送的 LSA 后，R3 实际上并没有向 R2 通告，这是因为 R3 并不知道网络中还有 R2 的存在。

14、要解决这样的问题，必须手工的指定网络的 DR 的角色。**由于 OSPF 的优先级会影响 DR 的选举，优先级为 0 的 OSPF 的路由永远不能成为 DR，优先级越高越容易成为 DR 的原则**，默认 OSPF 的优先级为 1，因此将 R2 与 R3 的优先级直接修改为 0，配置如下：

```
R2(config)#interface serial 1/2
R2(config-if)#ip ospf priority 0
R2(config-if)#exit
R2(config)#
```

```
R3(config)#interface serial 1/2
R3(config-if)#ip ospf priority 0
R3(config-if)#exit
```

15、查看所有路由器的邻居表，从邻居表可以看出 OSPF 各台路由器，已经拥有合适的角色：

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.3.1        0   FULL/DROTHER    00:00:38    192.168.1.2     Serial1/2
172.16.4.1        0   FULL/DROTHER    00:00:39    192.168.1.3     Serial1/2
R1#
```

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/DR         00:00:31    192.168.1.1     Serial1/2
R2#
```

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/DR         00:00:38    192.168.1.1     Serial1/2
R3#
```

16、其实也可以修改 OSPF 的接口类型，以避免 DR 和 BDR 的选举，从而减少 DR 选举出错的可能性。比如，将 R1 的接口网络类型修改为 P2MP（点到多点），而将 R2 和 R3 的接口网络类型修改为 P2P（点对点）。因为在 OSPF 的各种网络类型中：P2MP 和 P2P 都是不需要选举 DR 和 BDR 的。

17、另外，在配置接口网络类型时，还注意接口的 HELLO 死亡间隔时间。因为不同的类型的网络其时间是不一致的。**不一致的 HELLO 的时间间隔，会导致 OSPF 的邻居关系无法创建。**

18、下面给出一张 OSPF 所支持的网络类型和 DR 选举，以及 HELLO 时间间隔的表，以供参阅。具体配置不再列出。

OSPF Mode	NBMA Preferred Topology	Subnet Address	Hello Timer	Adjacency	RFC or Cisco
Broadcast	Full or partial mesh	Same	10 sec	Automatic, DR/BDR elected	Cisco
Nonbroadcast (NBMA)	Full or partial mesh	Same	30 sec	Manual configuration, DR/BDR elected	RFC
Point-to-multipoint	Partial-mesh or star	Same	30 Sec	Automatic, no DR/BDR	RFC
Point-to-multipoint nonbroadcast	partial-mesh or star	Same	30 sec	Manual configuration, no/DR/BDR	Cisco
Point-to-point	Partial-mesh or star, using subinterface	Different for Each Subinterface	10 sec	Automatic, no DR/BDR	Cisco

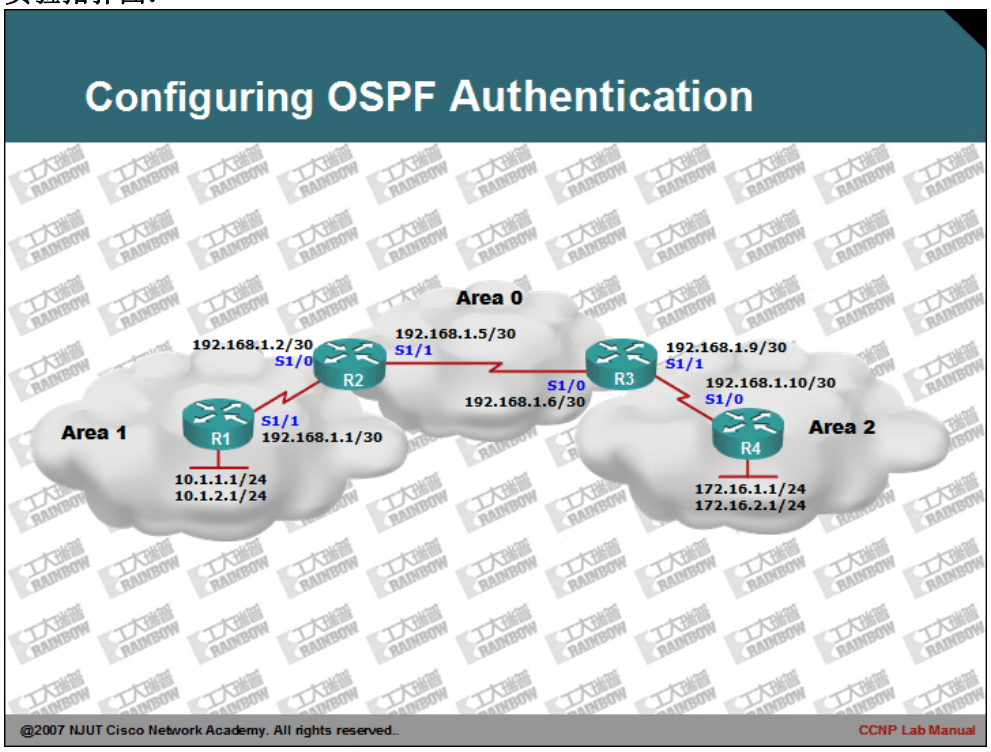
19、实验完成。

Lab 9. Configuring OSPF Authentication

实验目的：

1、掌握 OSPF 接口认证及区域认证的配置方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 OSPF 协议,并使用相关命令确认其正常工作。

3、查看 R1 和 R2 的路由表。

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
O IA    172.16.1.0 [110/193] via 192.168.1.2, 00:01:02, Serial1/1
O IA    172.16.2.0 [110/193] via 192.168.1.2, 00:01:02, Serial1/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback0
C       10.1.1.0 is directly connected, Loopback1
     192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/192] via 192.168.1.2, 00:01:12, Serial1/1
C       192.168.1.0 is directly connected, Serial1/1
O IA    192.168.1.4 [110/128] via 192.168.1.2, 00:05:47, Serial1/1
R1#
```

批注 [stanley92]: 通过 OSPF 协议学习到的其它区域的路由。

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
O IA    172.16.1.0 [110/129] via 192.168.1.6, 00:09:16, Serial1/1
O IA    172.16.2.0 [110/129] via 192.168.1.6, 00:09:16, Serial1/1
     10.0.0.0/24 is subnetted, 2 subnets
O       10.1.2.0 [110/65] via 192.168.1.1, 00:14:00, Serial1/0
O       10.1.1.0 [110/65] via 192.168.1.1, 00:14:00, Serial1/0
     192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/128] via 192.168.1.6, 00:09:26, Serial1/1
C       192.168.1.0 is directly connected, Serial1/0
C       192.168.1.4 is directly connected, Serial1/1
R2#
```

4、在 R1 上启用 OSPF 的明文认证，配置如下：

```
R1(config)#interface serial 1/1
R1(config-if)#ip ospf authentication
R1(config-if)#ip ospf authentication-key cisco
R1(config-if)#exit
```

批注 [stanley93]: 启用 OSPF 的认证。

批注 [stanley94]: 使用明文密码进行认证。

5、配置完成后，打开 debug 观察系统提示系统。

```
00:30:33: OSPF: 192.168.1.5 address 192.168.1.2 on Serial1/1 is dead
00:30:33: OSPF: 192.168.1.5 address 192.168.1.2 on Serial1/1 is dead, state DOWN
00:30:33: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.5 on Serial1/1 from FULL to DOWN, Neighbor
Down: Dead timer expired
00:30:35: OSPF: Rcv pkt from 192.168.1.2, Serial1/1 : Mismatch Authentication type. Input
packet specified type 0, we use type 1
00:54:45: OSPF: Rcv pkt from 192.168.1.2, Serial1/1 : Mismatch Authentication Key - Clear Text
```

批注 [stanley95]: 认证失败。导致邻居关系 down.

批注 [stanley96]: 此处信息指出 R1 配置的是明文的认证。

6、在 R2 上启用 OSPF 的认证：

```
R2(config)#interface s1/0
R2(config-if)#ip ospf authentication
R2(config-if)#ip ospf authentication-key cisco
R2(config-if)#exit
R2(config)#exit
```

7、查看 R1 的 debug 信息和路由表信息：

```
00:54:55: OSPF: 2 Way Communication to 192.168.1.5 on Serial1/1, state 2WAY
00:54:55: OSPF: Send DBD to 192.168.1.5 on Serial1/1 seq 0x2154 opt 0x42 flag 0x7 len 32
00:54:55: OSPF: Rcv DBD from 192.168.1.5 on Serial1/1 seq 0x182 opt 0x42 flag 0x7 len 32  mtu
1500 state EXSTART
00:54:55: OSPF: NBR Negotiation Done. We are the SLAVE
00:54:55: OSPF: Send DBD to 192.168.1.5 on Serial1/1 seq 0x182 opt 0x42 flag 0x2 len 152
00:54:55: OSPF: Rcv DBD from 192.168.1.5 on Serial1/1 seq 0x183 opt 0x42 flag 0x3 len 152  mtu
1500 state EXCHANGE
00:54:55: OSPF: Send DBD to 192.168.1.5 on Serial1/1 seq 0x183 opt 0x42 flag 0x0 len 32
00:54:55: OSPF: Database request to 192.168.1.5
00:54:55: OSPF: sent LS REQ packet to 192.168.1.2, length 60
00:54:55: OSPF: Rcv DBD from 192.168.1.5 on Serial1/1 seq 0x184 opt 0x42 flag 0x1 len 32  mtu
1500 state EXCHANGE
00:54:55: OSPF: Exchange Done with 192.168.1.5 on Serial1/1
00:54:55: OSPF: Send DBD to 192.168.1.5 on Serial1/1 seq 0x184 opt 0x42 flag
R1#0x0 len 32
00:54:55: OSPF: Synchronized with 192.168.1.5 on Serial1/1, state FULL
00:54:55: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.5 on Serial1/1 from LOADING to FULL, Loading
Done
00:54:56: OSPF: Build router LSA for area 1, router ID 10.1.2.1, seq 0x8000000C
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
O IA    172.16.1.0 [110/193] via 192.168.1.2, 00:01:53, Serial1/1
O IA    172.16.2.0 [110/193] via 192.168.1.2, 00:01:53, Serial1/1
```

```
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback0
C       10.1.1.0 is directly connected, Loopback1
     192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/192] via 192.168.1.2, 00:01:53, Serial1/1
C       192.168.1.0 is directly connected, Serial1/1
O IA    192.168.1.4 [110/128] via 192.168.1.2, 00:01:53, Serial1/1
R1#
```

批注 [stanley97]：由于认证成功。R1 再次学习到网络的路由。

8、另外：配置基于 MD5 的密码接口认证示例如下，配置完成后，请自行检查确认，此处不在重复确认过程：

```
R1(config)#interface serial 1/1
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
R1(config-if)#exit
R1(config)#
```

批注 [stanley98]：启用基于 md5 密码的认证。

批注 [stanley99]：设置认证密码。
其中数字 1 标识 key 的 id。最多可以设置 255 个密码。

```
R2(config)#interface serial 1/0
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco
R2(config-if)#exit
R2(config)#
```

9、no 掉之前配置的明文或是 md5 的接口认证。查看 R1 的路由表确认 OSPF 协议正常运行：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
O IA    172.16.1.0 [110/193] via 192.168.1.2, 00:00:05, Serial1/1
O IA    172.16.2.0 [110/193] via 192.168.1.2, 00:00:05, Serial1/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback0
C       10.1.1.0 is directly connected, Loopback1
     192.168.1.0/30 is subnetted, 3 subnets
O IA    192.168.1.8 [110/192] via 192.168.1.2, 00:00:05, Serial1/1
C       192.168.1.0 is directly connected, Serial1/1
O IA    192.168.1.4 [110/128] via 192.168.1.2, 00:00:05, Serial1/1
R1#
```

10、在 R1 上启用区域的明文认证，配置如下：

```
R1(config)#router ospf 1
R1(config-router)#area 1 authentication
```

批注 [stanley100]：为区域 1 启用 OSPF 的认证

```
R1(config-router)#exit
R1(config)#interface serial 1/1
R1(config-if)#ip ospf authentication-key cisco
R1(config-if)#exit
R1(config)#exit
```

批注 [stanley101]：在接口下配置区域认证的明文密码

11、在 R1 配置完成后，稍等几秒后，会在 R1 的路由器上出现如下信息：

```
01:10:25: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.5 on Serial1/1 from FULL to DOWN, Neighbor
Down: Dead timer expired
```

出现 down 的状态，是因为 R2 没有配置正确的认证。同时查看 R1 的路由表，发现之前学习的路由已丢失。

```
R1#show ip route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback0
C       10.1.1.0 is directly connected, Loopback1
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, Serial1/1
R1#
```

12、在 R2 上启用区域明文认证，配置如下：

```
R2(config)#router ospf 1
R2(config-router)#area 1 authentication
R2(config-router)#exit
R2(config)#interface serial 1/0
R2(config-if)#ip ospf authentication-key cisco
R2(config-if)#exit
```

批注 [stanley102]：为区域 1 启用 OSPF 的认证

批注 [stanley103]：在接口下配置区域认证的明文密码

13、在配置完 R2 的路由器的 OSPF 的区域明文认证后，随后在 R1 的路由器上会出现如下提示：

```
01:15:35: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.5 on Serial1/1 from LOADING to FULL, Loading
Done
```

此条信息指出，此时 OSPF 的认证成功，同时 R1 路由器已经学习到其它区域的路由。路由表显示如下：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
O IA    172.16.1.0 [110/193] via 192.168.1.2, 00:01:19, Serial1/1
```

```
O IA     172.16.2.0 [110/193] via 192.168.1.2, 00:01:19, Serial1/1
      10.0.0.0/24 is subnetted, 2 subnets
C        10.1.2.0 is directly connected, Loopback0
C        10.1.1.0 is directly connected, Loopback1
      192.168.1.0/30 is subnetted, 3 subnets
O IA     192.168.1.8 [110/192] via 192.168.1.2, 00:01:19, Serial1/1
C        192.168.1.0 is directly connected, Serial1/1
O IA     192.168.1.4 [110/128] via 192.168.1.2, 00:01:19, Serial1/1
R1#
```

14、另外：配置基于 MD5 的密码区域认证示例如下，配置完成后，请自行检查确认，此处不在重复确认过程：

```
R1(config)#router ospf 1
R1(config-router)#area 1 authentication message-digest
R1(config-router)#exit
R1(config)#interface serial 1/1
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
R1(config-if)#exit
R1(config)#
```

批注 [stanley104]：为区域启用基于 md5 的认证。

批注 [stanley105]：在接口下为区域认证配置 md5 的密码。

```
R2(config)#router ospf 1
R2(config-router)#area 1 authentication message-digest
R2(config-router)#exit
R2(config)#interface serial 1/0
R2(config-if)#ip ospf message-digest-key 1 md5 cisco
R2(config-if)#exit
R2(config)#
```

15、配置更改 md5 密码示例，此配置主要用于弃用旧密码，启用新密码时可能会使用（同样适用于区域的 md5 认证）：

```
R2(config)#interface serial 1/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco1
R2(config-if)#ip ospf message-digest-key 2 md5 cisco2
R2(config-if)#exit
R2(config)#exit
```

批注 [stanley106]：启用基于接口

批注 [stanley107]：当在接口出现两条 md5 的密码配置命令时，R2 路由会发送两份不同的分组数据包。分别使用 1 和 2 的密码。

一旦新的密码 2 可以使用了，原的密码 1 就可以使用 no 命令取消。完成旧密码到新密码的迁移。

16、实验完成。

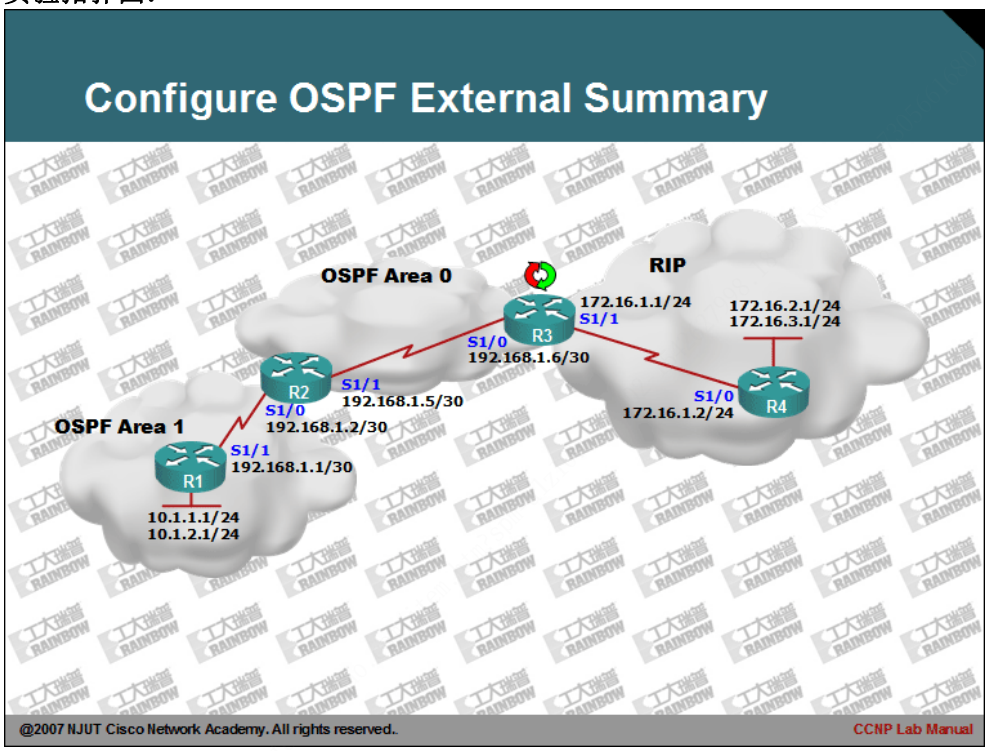
CCNP Lab Manual

Lab 10. Configuring OSPF External Summary

实验目的：

1、掌握 OSPF 外部路由汇总配置。
2、区别外部汇总的路由。
3、掌握 OSPF 的外部汇总路由类型及计算方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、R3(ASBR：自治系统边界路由器)路由器的配置。

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.1.4 0.0.0.3 area 0
R3(config-router)#exit
R3(config)#exit
R3#
R3(config)#router rip
R3(config-router)#network 172.16.0.0
R3(config-router)#exit
R3#
```

3、查看 R1 或是 R2 的路由表。

```
R1#show ip route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback1
C       10.1.1.0 is directly connected, Loopback0
     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial1/1
O IA    192.168.1.4 [110/128] via 192.168.1.2, 00:03:50, Serial1/1
R1#
```

4、在 R3 上配置重发布，(重发布的内容解释可以参考后面章节)。

```
R3(config)#router ospf 1
R3(config-router)#redistribute rip metric 200 subnets
R3(config-router)#exit
R3(config)#router rip
R3(config-router)#redistribute ospf 1 metric 10
R3(config-router)#exit
R3(config)#
```

批注 [stanley108]：将 rip 的路由重发布到 ospf 自治系统中。

批注 [stanley109]：将 ospf 自治系统路由重发布到 rip 网络中。

5、查看 R1 路由器路由表并使用 ping 命令确认路由。

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
O E1    172.16.1.0 [110/328] via 192.168.1.2, 00:04:22, Serial1/1
```

```
O E1    172.16.2.0 [110/328] via 192.168.1.2, 00:04:22, Serial1/1
O E1    172.16.3.0 [110/328] via 192.168.1.2, 00:04:22, Serial1/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback1
C       10.1.1.0 is directly connected, Loopback0
     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial1/1
O IA    192.168.1.4 [110/128] via 192.168.1.2, 00:16:54, Serial1/1
R1#
```

批注 [stanley110]：现在学习到的外网路由已经是 E1 的类型。
此时显示的 cost 值为 328，其中包含了到达 R3 的 cost。到达 R3 的 cost 值应为：328-200=128

批注 [stanley111]：此处显示的是到达 R3 的路由，其 cost 度量是 128。

通过上述比较，可以很清楚的理解 E1 与 E2 的路由度量计算方法。

9、查看 R1 路由器的链路状态数据库。

```
R1#show ip ospf database

            OSPF Router with ID (10.1.2.1) (Process ID 1)

                Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.2.1        10.1.2.1        1413        0x80000009 0x0003FD 4
192.168.1.5     192.168.1.5     1413        0x80000006 0x0025B8 2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.4     192.168.1.5     1437        0x80000001 0x00E33E

                Summary ASB Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.6     192.168.1.5     1061        0x80000001 0x00D348

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
172.16.1.0      192.168.1.6     3603        0x80000003 0x00CF35 0
172.16.2.0      192.168.1.6     3603        0x80000003 0x00C43F 0
172.16.3.0      192.168.1.6     3603        0x80000003 0x00B949 0
R1#
```

批注 [stanley112]：类型 4 的 LSA 用于指出 ASBR 位置。

批注 [stanley113]：类型 5 的 LSA 用于描述外网路由。

10、之前的 R1 的路由表中，显示的外网路由为 3 条。为了减少路由表的大小，可以在 R3 上进行外网的路由汇总，具体配置如下：

```
R3(config)#router ospf 1
R3(config-router)#summary-address 172.16.0.0 255.255.0.0
R3(config-router)#exit
R3(config)#exit
```

批注 [stanley114]：对 RIP 的网络进行汇总。

11、查看 R1 路由表，确认汇总成功。

```
R1#show ip route

Gateway of last resort is not set

O E1 172.16.0.0/16 [110/328] via 192.168.1.2, 00:01:29, Serial1/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, Loopback1
C       10.1.1.0 is directly connected, Loopback0
     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial1/1
O IA    192.168.1.4 [110/128] via 192.168.1.2, 00:24:56, Serial1/1
R1#
```

批注 [stanley115]: 此处显示的路由，已经表明汇总成功。

12、完成实验。

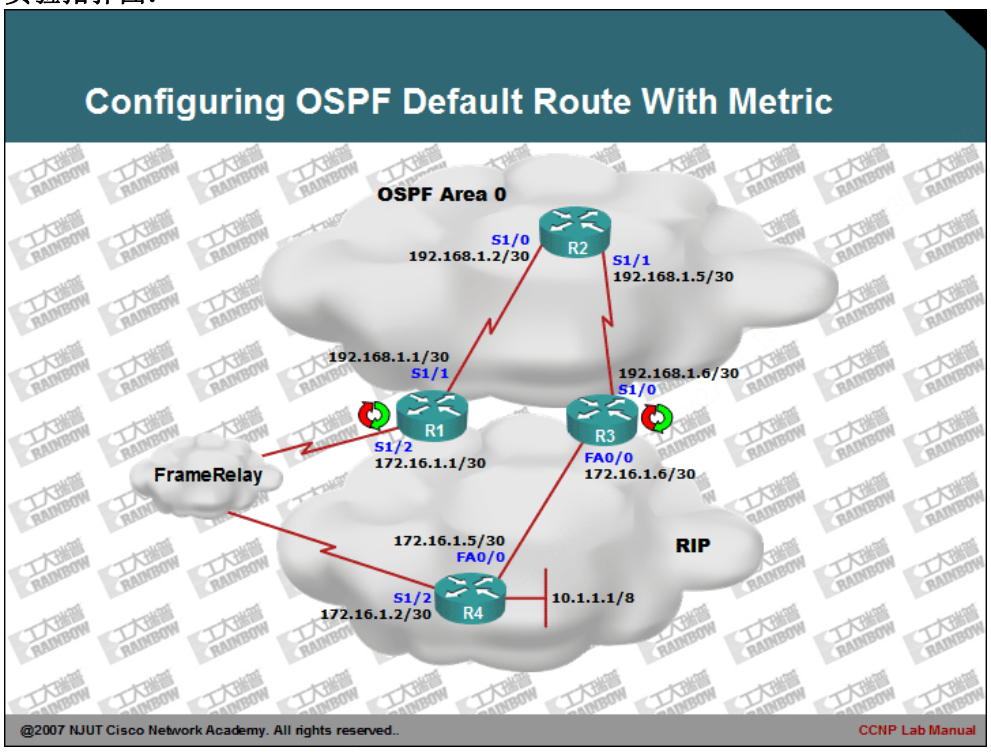
CCNP Lab Manual

Lab 11. Configuring OSPF Default Route With Metric

实验目的：

1、掌握如何使用管理距离控制 OSPF 的默认路由选择。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、R1 与 R4 路由器的 s1/2 接口帧中继配置。

```
R1(config)#interface serial 1/2
R1(config-if)#encapsulation frame-relay
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config)#exit
```

批注 [stanley116]：启用帧中继封装

```
R4(config)#interface serial 1/2
R4(config-if)#encapsulation frame-relay
R4(config-if)#ip address 172.16.1.2 255.255.255.252
R4(config)#exit
```

批注 [stanley117]：启用帧中继封装

3、按实验拓扑配置各路由器的 OSPF 协议，注意接口所在不同网络。

4、查看 R2 的路由表。

```
R2#show ip route

Gateway of last resort is not set

     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial1/0
C       192.168.1.4 is directly connected, Serial1/1
R2#
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2#
```

批注 [stanley118]：此时无法 ping 通 rip 网络中 10.1.1.1/8 的地址.

5、为了能够保证网络通讯，在 R1 和 R3 上配置不同协议的路由重发布和 OSPF 的默认路由。

```
R1(config)#router rip
R1(config-router)#redistribute ospf 1 metric 10
R1(config-router)#exit
R1(config)#
R1(config)#router ospf 1
R1(config-router)# default-information originate always
R1(config-router)#exit
```

批注 [stanley119]：向 OSPF 网络通告默认路由。使用 always 参数的目的是：在没有配置静态默认路由的情况下始终向 OSPF 网络通告默认路由。

```
R1(config)#exit
```

```
R3(config)#router rip
R3(config-router)#redistribute ospf 1 metric 10
R3(config-router)#exit
R3(config)#
R3(config)#router ospf 1
R3(config-router)# default-information originate always
R3(config-router)#exit
R3(config)#exit
R3#
```

6、再次查看 R2 路由器路由表并使用 ping 命令确认路由。

```
R2#show ip route

Gateway of last resort is not set

O E2 10.0.0.0/8 [110/20] via 192.168.1.1, 00:01:19, Serial1/0
     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial1/0
C       192.168.1.4 is directly connected, Serial1/1
O*E2 0.0.0.0/0 [110/1] via 192.168.1.6, 00:01:19, Serial1/1
                [110/1] via 192.168.1.1, 00:01:19, Serial1/0
R2#
R2#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/82/120 ms
R2#
```

批注 [stanley120]：由于同时从 R1 和 R3 上学习默认路由，因此 R2 采用均衡负载方式进行了转发到达外网的数据包。

7、在上面的实验中，R2 选择到达非 OSPF 网络的路由下一跳是 R1 和 R3，并且是均衡负载。而在本实验中，从 R1 到达非 OSPF 网络是使用帧中继的网络。从 R3 到达非 OSPF 网络是使用 100Mbps 的快速以太网。因此选择从 R3 到达外网远比从 R1 到达非 OSPF 网络要好。也即是最佳最路由。

8、为了解决这个问题，在通告默认路由时可以采用定制度量的参数，来影响路由器选择最佳路由。可以在 R1 和 R3 上进行如下配置。

```
R1(config)#router ospf 1
R1(config-router)#default-information originate always metric 100
```

批注 [stanley121]：在 R1 上配置通告的默认路由度量值是 100。

```
R1(config-router)#exit
```

```
R3(config)#router ospf 1
R3(config-router)#default-information originate always metric 50
R3(config-router)#exit
```

批注 [stanley122]：在 R1 上配置通告的默认路由度量值是 50。

9、再次查看 R2 的路由表。

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.6 to network 0.0.0.0

O E2 10.0.0.0/8 [110/20] via 192.168.1.1, 00:08:05, Serial1/0
     192.168.1.0/30 is subnetted, 2 subnets
C       192.168.1.0 is directly connected, Serial1/0
C       192.168.1.4 is directly connected, Serial1/1
O*E2 0.0.0.0/0 [110/50] via 192.168.1.6, 00:00:32, Serial1/1
R2#
```

批注 [stanley123]：此时 R2 已经选择从 R3 到达非 OSPF 的网络。

10、此时非最佳路由的问题已经解决。**其实更准确的说，是通过控制 OSPF 的默认路由的度量值，来影响 OSPF 路由器选择最佳路由。**

11、实验完成。

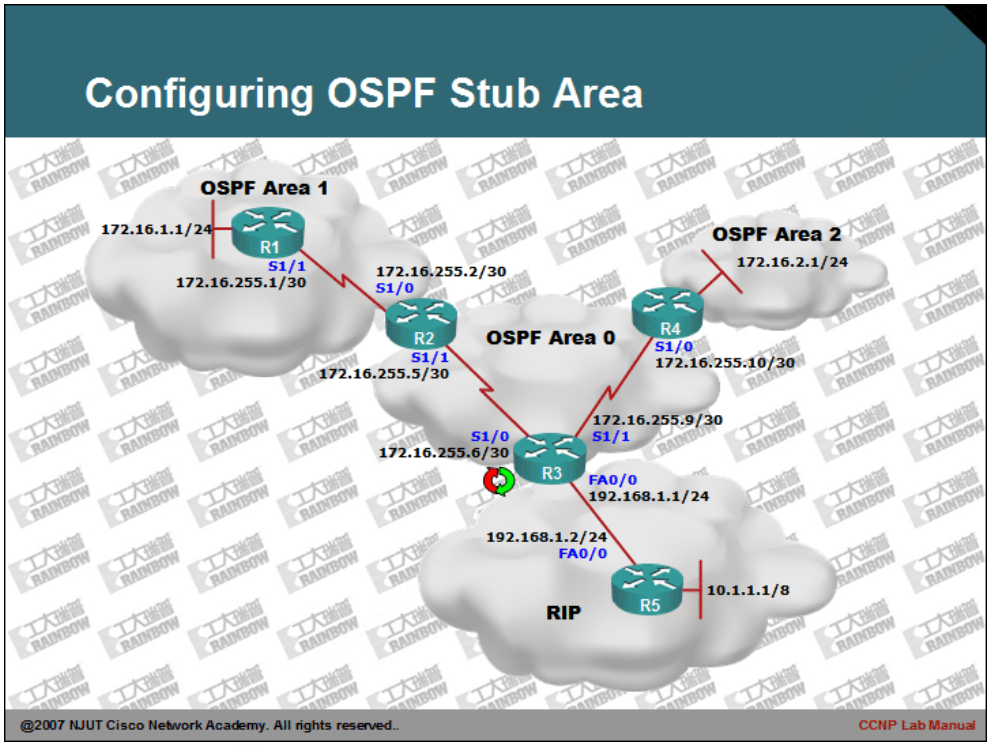
CCNP Lab Manual

Lab 12. Configuring OSPF Stub Area

实验目的：

1、掌握类型 1、2、3、4 和 5 的 LSA 的作用。
2、掌握 OSPF 末节（Stub）区域特点。
3、掌握 OSPF Stub 区域配置方法。
4、掌握 OSPF Stub 区域配置要求：**Stub 区域没有 ASBR，它至少拥有一个 ABR。**

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 OSPF 与 RIP 的协议，并使用 ping 和 show ip route 命令进行确认协议正常工作。

3、为了完成实验需要在 R3 上配置重发布，配置如下：

```
R3(config)#router ospf 1
R3(config-router)#redistribute rip subnets metric 200
R3(config-router)#exit
R3(config)#
R3(config)#router rip
R3(config-router)#redistribute ospf 1 metric 10
R3(config-router)#exit
R3(config)#exit
```

4、查看 R1 路由器的路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
O IA    172.16.255.4/30 [110/128] via 172.16.255.2, 00:07:32, Serial1/1
O IA    172.16.255.8/30 [110/192] via 172.16.255.2, 00:06:57, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
O IA    172.16.2.0/24 [110/193] via 172.16.255.2, 00:06:05, Serial1/1
O E2 10.0.0.0/8 [110/200] via 172.16.255.2, 00:02:01, Serial1/1
O E2 192.168.1.0/24 [110/200] via 172.16.255.2, 00:02:01, Serial1/1
R1#
R1#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 672/788/984 ms
R1#
```

批注 [stanley124]： IA 类型路由是由LSA3通告的区域间路由。

批注 [stanley125]： E2 类型路由是由LSA5通告的外部区域路由。

5、查看 R1 路由器的链路状态数据库。

```
R1#show ip ospf database

            OSPF Router with ID (172.16.1.1) (Process ID 1)
```

```
                Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.1.1      172.16.1.1      682         0x80000003 0x003BE1 3
172.16.255.5    172.16.255.5    677         0x80000003 0x0035B1 2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.2.0      172.16.255.5    581         0x80000001 0x004CEE
172.16.255.4    172.16.255.5    668         0x80000001 0x009BE1
172.16.255.8    172.16.255.5    633         0x80000001 0x00F543

                Summary ASB Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.1     172.16.255.5    342         0x80000001 0x008648

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
10.0.0.0        192.168.1.1     348         0x80000001 0x005B1B 0
192.168.1.0     192.168.1.1     348         0x80000001 0x0021F4 0
R1#
```

批注 [stanley126]：类型 1 的 LSA 用于宣告具体网络。

批注 [stanley127]：类型 3 的 LSA 用于宣告区域间路由。

批注 [stanley128]：类型 4 的 LSA 用于指出自治系统边界路由器(ASBR)的位置。

批注 [stanley129]：类型 5 的 LSA 用于宣告外部路由。

6、我们注意到 R1 路由学习到的本次实验拓扑中所有的路由，在实际网络应用中，R1 路由并不需要学习到整个网络路由。过多的路由条目会导致路由器变大，不利用路由查询，同时也不利于网络的收敛。OSPF 网络路由是通过 LSA 来进行通告。可以**限制 LSA 的泛洪的范围，并辅以适当的汇总路由，从而有效的减少路由表的大小，便于网络的收敛，同时增强网络稳定性**。

7、在 R1 和 R2 上配置 area 1 区域为 stub 区域。

```
R1(config)#router ospf 1
R1(config-router)#area 1 stub
R1(config-router)#exit
R1(config)#exit
```

批注 [stanley130]：配置 area 1 区域为末节区域。同时需要注意的是：只要是从属于 area 1 区域的 OSPF 路由器，都需要配置此命令。

```
R2(config)#router ospf 1
R2(config-router)#area 1 stub
R2(config-router)#exit
R2(config)#
```

批注 [stanley131]：在 ABR 上即 R2 路由器配置指出 area 1 为末节区域。

8、再次查看 R1 的链路状态数据库。

```
R1#show ip ospf database

            OSPF Router with ID (172.16.1.1) (Process ID 1)
```

```
                Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.1.1      172.16.1.1      155         0x80000005 0x0055C7 3
172.16.255.5    172.16.255.5    155         0x80000005 0x004F97 2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.0         172.16.255.5    168         0x80000001 0x00017B
172.16.2.0      172.16.255.5    168         0x80000002 0x0068D3
172.16.255.4    172.16.255.5    168         0x80000002 0x00B7C6
172.16.255.8    172.16.255.5    168         0x80000002 0x001228
R1#
```

批注 [stanley132]: 由于在 R2 上配置 area 1 为末节区域。
因此 R2 必须发送一条默认路由以确保 area 1 区域的路由器通过访问非 OSPF 的网络。

通过查看 R1 的数据库，可以发现类型 4 和 5 的 LSA 被拒绝了，从而限制了 LSA 的泛洪范围。

9、查看 R1 的路由表，确认路由表变化。因为有 R2 发送的默认路由，因此 R1 也不需要接收类型 3 的 LSA，即无需要知晓 ASBR 的位置。

```
R1#show ip route

Gateway of last resort is 172.16.255.2 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
O IA    172.16.255.4/30 [110/128] via 172.16.255.2, 00:04:19, Serial1/1
O IA    172.16.255.8/30 [110/192] via 172.16.255.2, 00:04:19, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
O IA    172.16.2.0/24 [110/193] via 172.16.255.2, 00:04:19, Serial1/1
O*IA 0.0.0.0/0 [110/65] via 172.16.255.2, 00:04:19, Serial1/1
R1#
```

批注 [stanley133]: R2 发送的默认路由。

10、使用 ping 命令确认路由有效性。

```
R1#ping 10.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 240/393/684 ms
R1#
```

11、通过以上配置，需要掌握的是：末节区域（stub area）拒绝了类型 4 和类型 5 的 LSA。

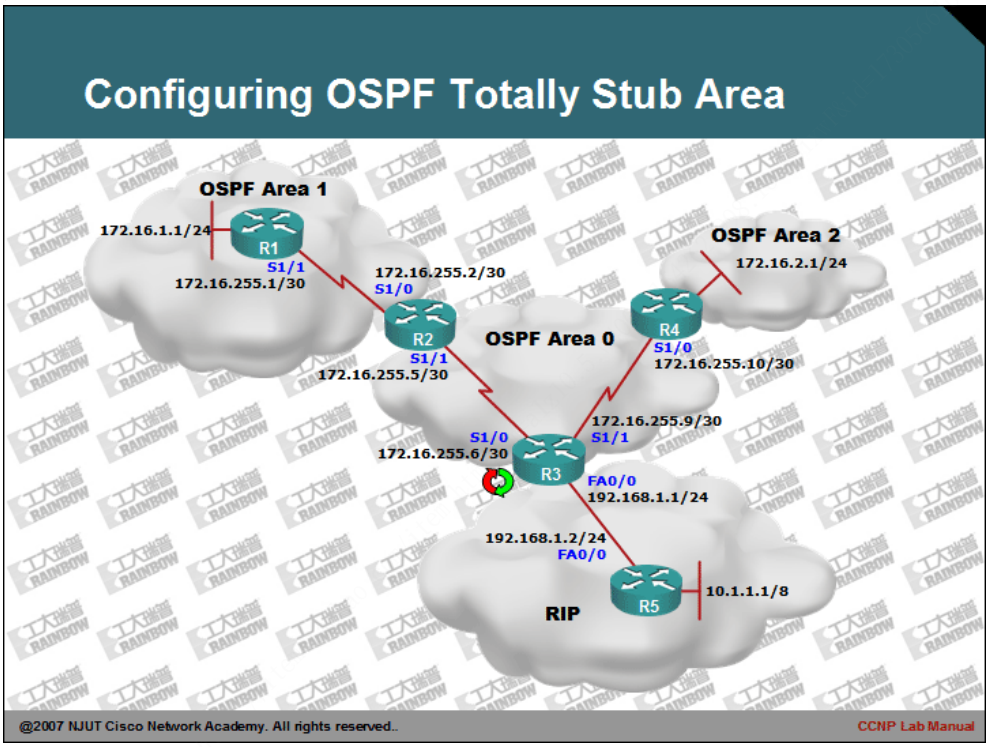
12、实验完成。

Lab 13. Configuring OSPF Totally Stub Area

实验目的：

1、掌握类型 1、2、3、4 和 5 的 LSA 的作用。
2、掌握 OSPF 完全末节（Totally Stub）区域特点。
3、掌握 OSPF Totally Stub 区域配置方法。
4、掌握 OSPF Stub 区域配置要求：**Stub 区域没有 ASBR，它至少拥有一个 ABR。**
5、**注意：完全末节区域(NSSA)为 CISCO 私有的。**

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 OSPF 与 RIP 的协议，并使用 ping 和 show ip route 命令进行确认协议正常工作。

3、为了完成实验需要在 R3 上配置重发布，配置如下:

```
R3(config)#router ospf 1
R3(config-router)#redistribute rip subnets metric 200
R3(config-router)#exit
R3(config)#
R3(config)#router rip
R3(config-router)#redistribute ospf 1 metric 10
R3(config-router)#exit
R3(config)#exit
```

4、**首先将 area 1 配置成 ospf stub area 区域。**

5、查看 R1 路由器的路由表和数据链路状态数据库。

```
R1#show ip ospf database

            OSPF Router with ID (172.16.1.1) (Process ID 1)

                Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.1.1      172.16.1.1      155         0x80000005 0x0055C7 3
172.16.255.5    172.16.255.5    155         0x80000005 0x004F97 2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.0         172.16.255.5    168         0x80000001 0x00017B
172.16.2.0      172.16.255.5    168         0x80000002 0x0068D3
172.16.255.4    172.16.255.5    168         0x80000002 0x00B7C6
172.16.255.8    172.16.255.5    168         0x80000002 0x001228
R1#
R1#show ip route

Gateway of last resort is 172.16.255.2 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
O IA    172.16.255.4/30 [110/128] via 172.16.255.2, 00:04:19, Serial1/1
```

```
O IA    172.16.255.8/30 [110/192] via 172.16.255.2, 00:04:19, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
O IA    172.16.2.0/24 [110/193] via 172.16.255.2, 00:04:19, Serial1/1
O*IA 0.0.0.0/0 [110/65] via 172.16.255.2, 00:04:19, Serial1/1
R1#
```

批注 [stanley134]: R2 发送的默认路由。

6、通过 stub 的区域特性配置，已经可以有效的减少路由表的大小。但是此时 R1 的路由表并不是最精简的。可以使用 totally stub 区域特性来进一步的减少路由表尺寸。配置如下：

```
R2(config)#router ospf 1
R2(config-router)#area 1 stub no-summary
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley135]: 使用 no-summary 命令可以拒绝类型 3 的 LSA 泛洪到 area 1 区域。

```
R1(config)#router ospf 1
R1(config-router)#area 1 stub
R1(config-router)#exit
R1(config)#exit
R1#
```

批注 [stanley136]: Area 1 区域的路由器需要指定为末节区域特性。

7、再次查看 R1 的路由表。

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.255.2 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
O*IA 0.0.0.0/0 [110/65] via 172.16.255.2, 00:34:32, Serial1/1
R1#
```

批注 [stanley137]: 通过配置完全末节特性，现在 R1 路由器只剩下默认路由。

8、查看 R1 的链路状态数据库。现在 R1 的链路状态数据库，仅有类型 1 和经过汇总的类型 3 的 LSA。而其它的 OSPF 区域 LSA 被禁止了。

```
R1#show ip ospf database
```

```
            OSPF Router with ID (172.16.1.1) (Process ID 1)

                Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.1.1      172.16.1.1      387         0x80000006 0x0053C8 3
172.16.255.5    172.16.255.5    412         0x80000006 0x004D98 2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.0         172.16.255.5    295         0x80000003 0x00FC7D
R1#
```

9、使用 ping 命令确认路由。

```
R1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 216/570/1488 ms
R1#
```

10、本次实验的关键是：**完全末节区域(Totally Stub Area)拒绝了类型 3、类型 4 和类型 5 的 LSA。而对于其它区域的非 OSPF 自治系统的网络使用默认路由替代。**

11、实验完成。

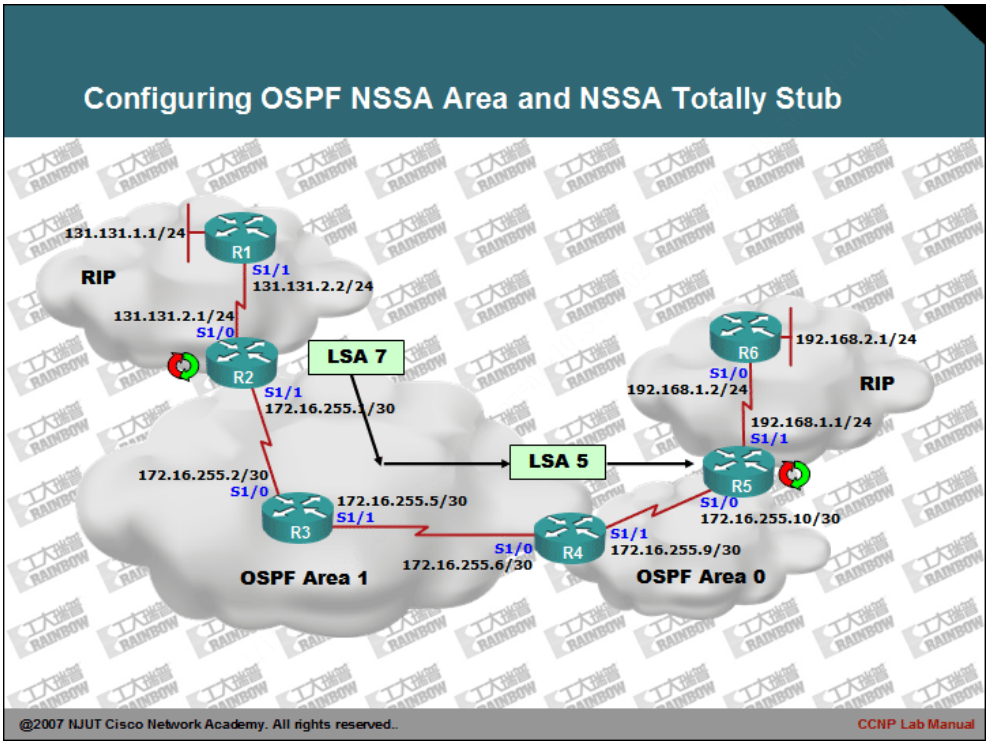
CCNP Lab Manual

Lab 14. Configuring OSPF NSSA Area and NSSA Totally Stub

实验目的：

1、掌握类型 1、2、3、4 和 5 的 LSA，及**类型 7 的 LSA 在完全次末节区域的作用**。
2、掌握次末节区域（NSSA）和完全次末节区域(NSSA Totally Stub Area)特点。
3、掌握两种区域配置方法。
4、注意：完全次末节区域(Totally NSSA)为 CISCO 私有的。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 OSPF 与 RIP 的协议，并使用 ping 和 show ip route 命令进行确认协议正常工作。

3、为了完成实验需要在 R2 和 R5 上配置重发布，配置如下：

```
R2(config)#router ospf 1
R2(config-router)#redistribute rip metric 200 subnets
R2(config-router)#exit
R2(config)#
R2(config)#router rip
R2(config-router)#redistribute ospf 1 metric 10
R2(config-router)#exit
R2(config)#exit
```

```
R5(config)#router ospf 1
R5(config-router)#redistribute rip metric 200 subnets
R5(config-router)#exit
R5(config)#
R5(config)#router rip
R5(config-router)#redistribute ospf 1 metric 10
R5(config-router)#exit
R5(config)#exit
```

4、查看 R3 的路由表的路由表和链路状态数据库。

```
R3#show ip ospf database

            OSPF Router with ID (172.16.255.5) (Process ID 1)

                Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.255.1    172.16.255.1    534         0x80000005 0x008564 2
172.16.255.5    172.16.255.5    679         0x80000004 0x007390 4
172.16.255.9    172.16.255.9    672         0x80000003 0x00A42F 2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.255.8    172.16.255.9    662         0x80000001 0x005B1A

                Summary ASB Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
```

批注 [stanley138]: 用于描述其它 OSPF 区域的 LSA 3

```
192.168.1.1       172.16.255.9     98          0x80000001 0x006E5C

                  Type-5 AS External Link States
Link ID           ADV Router       Age         Seq#       Checksum Tag
131.131.1.0       172.16.255.1     513         0x80000001 0x007BAA 0
131.131.2.0       172.16.255.1     513         0x80000001 0x0070B4 0
192.168.1.0       192.168.1.1      94          0x80000002 0x001FF5 0
192.168.2.0       192.168.1.1      94          0x80000002 0x0014FF 0
R3#
```

批注 [stanley139]：由 R2 通告的用于描述外部网络路由的 LSA 5

批注 [stanley140]：从 R5 通告的用于描述外部网络路由的 LSA 5

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.255.0 is directly connected, Serial1/0
C       172.16.255.4 is directly connected, Serial1/1
O IA    172.16.255.8 [110/128] via 172.16.255.6, 00:07:46, Serial1/1
     131.131.0.0/24 is subnetted, 2 subnets
O E2    131.131.1.0 [110/200] via 172.16.255.1, 00:00:30, Serial1/0
O E2    131.131.2.0 [110/200] via 172.16.255.1, 00:00:30, Serial1/0
O E2 192.168.1.0/24 [110/200] via 172.16.255.6, 00:00:30, Serial1/1
O E2 192.168.2.0/24 [110/200] via 172.16.255.6, 00:00:30, Serial1/1
R3#
```

批注 [stanley141]：R3 路由学习到多个区域和多个非 OSPF 的网络路由。

4、**由于 area 1 路由违背了 stub 区域要求，即 stub 区域不能够有 ASBR 路由器的特性。**因此本实验采用 NSSA 的配置方法来减少 R3 路由器的路由表大小。

5、在 R4 上将 area 1 区域配置成 NSSA 区域：

```
R4(config)#router ospf 1
R4(config-router)#area 1 nssa default-information-originate
R4(config-router)#exit
R4(config)#
```

批注 [stanley142]：指出 area 1 为 NSSA 区域。Default-information-originate 的参数目的是向 area 1 区域注入一条默认路由。

6、在 R3 上作如下配置。

```
R3(config)#router ospf 1
R3(config-router)#area 1 nssa
R3(config-router)#exit
R3(config)#exit
R3#
```

批注 [stanley143]：指出自己所在区域是 NSSA 区域。

7、在 R2 上作如下配置。

```
R2(config)#router ospf 1
R2(config-router)#area 1 nssa
R2(config-router)#exit
```

批注 [stanley144]：指出 area 1 所在区域是 NSSA 区域。

```
R2(config)#exit
R3#
```

8、再次查看 R3 路由表和链路状态数据库。

```
R3#show ip route
Gateway of last resort is 172.16.255.6 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.255.0 is directly connected, Serial1/0
C       172.16.255.4 is directly connected, Serial1/1
O IA    172.16.255.8 [110/128] via 172.16.255.6, 00:01:10, Serial1/1
     131.131.0.0/24 is subnetted, 2 subnets
O N2    131.131.1.0 [110/200] via 172.16.255.1, 00:01:10, Serial1/0
O N2    131.131.2.0 [110/200] via 172.16.255.1, 00:01:10, Serial1/0

O*N2 0.0.0.0/0 [110/1] via 172.16.255.6, 00:01:10, Serial1/1
R3#
```

批注 [stanley145]: OSPF 区域间路由

批注 [stanley146]: 从 R2 路由获得的外网路由。

批注 [stanley147]: 本条默认路由用于指出如何到达 R5 路由器所连接的外网。

如果：R5 所连接的外部网络路由较多时，这样的做的好外是不言而喻的。

下面显示的是 R3 的链路状态数据库。

```
R3#show ip ospf database

            OSPF Router with ID (172.16.255.5) (Process ID 1)

                Router Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.255.1    172.16.255.1    314         0x80000007 0x0027BA 2
172.16.255.5    172.16.255.5    314         0x80000008 0x0011E8 4
172.16.255.9    172.16.255.9    450         0x80000005 0x004C7D 2

                Summary Net Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum
172.16.255.8    172.16.255.9    850         0x80000002 0x00FE6F

                Type-7 AS External Link States (Area 1)

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.16.255.9    850         0x80000001 0x00C464 0
131.131.1.0     172.16.255.1    318         0x80000001 0x00213D 0
131.131.2.0     172.16.255.1    318         0x80000001 0x001647 0
R3#
```

批注 [stanley148]: 到达 R5 所连接的网络，由默认路由替代。

9、查看 R2 或 R3 的路由表。

```
R2#show ip route
```

```
Gateway of last resort is 172.16.255.2 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.255.0 is directly connected, Serial1/1
O       172.16.255.4 [110/128] via 172.16.255.2, 00:07:26, Serial1/1
O IA    172.16.255.8 [110/192] via 172.16.255.2, 00:07:26, Serial1/1
     131.131.0.0/24 is subnetted, 2 subnets
R       131.131.1.0 [120/1] via 131.131.2.2, 00:00:06, Serial1/0
C       131.131.2.0 is directly connected, Serial1/0
O*N2 0.0.0.0/0 [110/1] via 172.16.255.2, 00:07:26, Serial1/1
R2#
```

批注 [stanley149]：R2 也成功学习到默认路由。

下面是 R1 路由器的路由表内容：

```
R1#show ip route
Gateway of last resort is 131.131.2.1 to network 0.0.0.0
R    172.16.0.0/16 [120/10] via 131.131.2.1, 00:00:28, Serial1/1
     131.131.0.0/24 is subnetted, 2 subnets
C       131.131.1.0 is directly connected, Loopback0
C       131.131.2.0 is directly connected, Serial1/1
R*   0.0.0.0/0 [120/10] via 131.131.2.1, 00:00:28, Serial1/1
R1#
```

批注 [stanley150]：R1 通过 R2 的重发布，正确学习到默认路由。

10、在 R1 上使用 ping 命令测试默认路由有效性：

```
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 288/384/432 ms
R1#
```

批注 [stanley151]：结果显示默认路由是可用的。

11、为了进一步简化 area 1 区域的路由器的路由表，我们采用完全次末节区域（Totally NSSA）特性来配置 area 1。

12、在 NSSA 的基础上配置 Totally NSSA 区域特性，只需要在 R4 的路由器上作如下配置：

```
R4(config)#router ospf 1
R4(config-router)#area 1 nssa no-summary
R4(config-router)#exit
```

批注 [stanley152]：配置 area1 为完全次末节区域。

no-summary 参数指出：不要向区域 1 发送类型 3 的区域间汇总路由。

13、再次查看 R3 的路由表和链路状态数据库：

```
R3#show ip route

Gateway of last resort is 172.16.255.6 to network 0.0.0.0
```

```
     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.255.0 is directly connected, Serial1/0
C       172.16.255.4 is directly connected, Serial1/1
     131.131.0.0/24 is subnetted, 2 subnets
O N2    131.131.1.0 [110/200] via 172.16.255.1, 00:20:24, Serial1/0
O N2    131.131.2.0 [110/200] via 172.16.255.1, 00:20:24, Serial1/0
O*IA 0.0.0.0/0 [110/65] via 172.16.255.6, 00:02:10, Serial1/1
R3#
```

批注 [stanley153]：到达其它 OSPF 区域和非 R2 路由器通告的外网路由均被此条默认替代。

更精简有效的路由表条目。

```
R3#show ip ospf database
            OSPF Router with ID (172.16.255.5) (Process ID 1)

                Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.255.1    172.16.255.1    1504        0x80000007 0x0027BA 2
172.16.255.5    172.16.255.5    1504        0x80000008 0x0011E8 4
172.16.255.9    172.16.255.9    1640        0x80000005 0x004C7D 2

                Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
0.0.0.0         172.16.255.9    396         0x80000001 0x0070FF

                Type-7 AS External Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         172.16.255.9    66          0x80000002 0x00C265 0
131.131.1.0     172.16.255.1    1508        0x80000001 0x00213D 0
131.131.2.0     172.16.255.1    1508        0x80000001 0x001647 0
R3#
```

批注 [stanley154]：因为完全次末节区域与完全末节区域类似的是：**丢弃类型 3 和类型 4 以及类型 5 的 LSA。**

所以此外将默认路由转发类型 7，以便向 R2 进行通告。

批注 [stanley155]：从 R2 路由器收到的类型 7 的 LSA。

此类型的 LSA 在送达到区域边界路由器（ABR），本例中即 R4 后，R4 会将其转换为类型 5 的 LSA 转发给其它区域路由。

14、查看 R1 和 R2 路由表，并且使用 ping 命令确认路由。

```
R2#show ip route

Gateway of last resort is 172.16.255.2 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.255.0 is directly connected, Serial1/1
O       172.16.255.4 [110/128] via 172.16.255.2, 00:23:09, Serial1/1
     131.131.0.0/24 is subnetted, 2 subnets
R       131.131.1.0 [120/1] via 131.131.2.2, 00:00:17, Serial1/0
C       131.131.2.0 is directly connected, Serial1/0
O*IA 0.0.0.0/0 [110/129] via 172.16.255.2, 00:04:46, Serial1/1
R2#
```

```
R1#show ip route
```

```
Gateway of last resort is 131.131.2.1 to network 0.0.0.0

R    172.16.0.0/16 [120/10] via 131.131.2.1, 00:00:13, Serial1/1
     131.131.0.0/24 is subnetted, 2 subnets
C       131.131.1.0 is directly connected, Loopback0
C       131.131.2.0 is directly connected, Serial1/1
R*   0.0.0.0/0 [120/10] via 131.131.2.1, 00:00:13, Serial1/1
R1#
```

```
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 336/454/528 ms
R1#
```

15、最后，到 R5 的路由器上查看在 R3 路由器上的类型 7 的 LSA 是否被转换为类型 5 的 LSA：

```
R5#show ip ospf database

            OSPF Router with ID (192.168.1.1) (Process ID 1)

                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
172.16.255.9    172.16.255.9    338         0x80000004 0x005DC2 2
192.168.1.1     192.168.1.1     767         0x80000004 0x002753 2

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.255.0    172.16.255.9    81          0x80000002 0x002C10
172.16.255.4    172.16.255.9    1337        0x80000002 0x0081F6

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
131.131.1.0     172.16.255.9    1761        0x80000001 0x0085DA 0
131.131.2.0     172.16.255.9    1761        0x80000001 0x007AE4 0
192.168.1.0     192.168.1.1     767         0x80000003 0x001DF6 0
192.168.2.0     192.168.1.1     767         0x80000003 0x001201 0
R5#
```

批注 [stanley156]： 在 R5 上发现了描述 131.31.0.0/16 网络的类型 5 的 LSA。

说明：R4 确实将 R3 发送给 R4 的类型 7 的 LSA 转换为类型 5 的 LSA 向其它区域路由转发了。

16、实验完成。

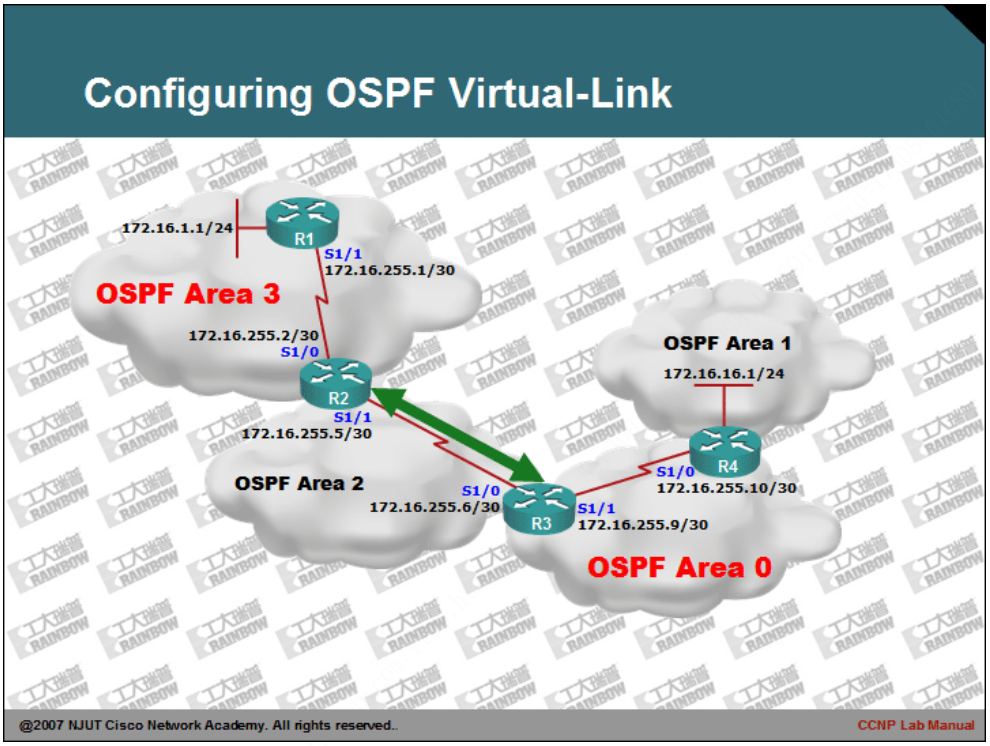
Lab 15. Configuring OSPF Virtual-Link

实验目的：

1、理解 OSPF 虚链路原理及何时需要使用虚链路。

2、掌握 OSPF 虚链路配置方法

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、首先配置 R2,R3,R4 的 OSPF 协议，配置过程中注意区域号，**另外：在 R2 的 OSPF 协议中先不要 network s1/0 接口 IP 标识**。确保 area 2 、area 0 和 area 1 的 OSPF 能够正常工作。其中 R2 路由的 OSPF 配置如下如示：

```
R2(config)#router ospf 1
R2(config-router)#network 172.16.255.4 0.0.0.3 area 2
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley157]：首先只需要 network s1/1 接口的网络。

3、查看 R2 的路由表。

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/0
C       172.16.255.4/30 is directly connected, Serial1/1
O IA    172.16.255.8/30 [110/128] via 172.16.255.6, 00:00:27, Serial1/1
O IA    172.16.16.1/32 [110/129] via 172.16.255.6, 00:00:04, Serial1/1
R2#
```

4、再次配置 R1 和 R2 的 OSPF 协议，配置如下：

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.255.0 0.0.0.3 area 3
R1(config-router)#network 172.16.1.0 0.0.0.255 area 3
R1(config-router)#exit
R1(config)#exit
R1#
```

```
R2(config)#router ospf 1
R2(config-router)#network 172.16.255.0 0.0.0.3 area 3
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley158]：完成对 R2 的 s1/0 接口的配置。

5、查看 R1 与 R2 的 OSPF 的邻居表：

```
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.255.5      1   FULL/  -        00:00:38    172.16.255.2    Serial1/1
```

批注 [stanley159]：Full 的关键字指出已经成功与 R2 路由器创建邻居关系。

```
R1#
```

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.255.9      1   FULL/  -        00:00:37    172.16.255.6    Serial1/1
172.16.1.1        1   FULL/  -        00:00:30    172.16.255.1    Serial1/0
R2#
```

批注 [stanley160]：与 R1 创建邻居关系成功。

6、查看 R1 路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
R1#
```

通过观察 R1 的路由表，R1 的路由器无法学习到骨干区域、area 1 和 area 2 区域的路由。**造成这个问题的主要原因是：area 3 区域与骨干区域 area 0 被分割。OSPF 的区域配置规则是：普通区域必须与骨干区域直连。**

7、当有这种问题出现时，可以使用虚链路的配置方案解决。使用虚链路可以确保非直连区域能够逻辑认为自己与骨干区域直连。在 R2 和 R3 上进行如下虚拟路的配置。

```
R2(config)#router ospf 1
R2(config-router)#area 2 virtual-link 172.16.255.9
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley161]：创建虚链路。

命令中的 area 2 指出有一条虚链路存在于区域 2 中。virtual-link 172.16.255.9 指出创建虚链路的**对端 R3 路由器的 router id。**

```
R3(config)#router ospf 1
R3(config-router)#area 2 virtual-link 172.16.255.5
R3(config-router)#exit
R3(config)#exit
R3#
```

批注 [stanley162]：配置到 R2 路由器虚链路。
注意：使用 router id，而不是接口 ip.

8、查看 R2 的邻居表：

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.255.9      1   FULL/  -        00:00:30    172.16.255.6    Serial1/1
172.16.1.1        1   FULL/  -        00:00:33    172.16.255.1    Serial1/0
```

批注 [stanley163]：已经与 R3 路由器创建邻居关系。

```
R2#
```

9、查看 R2 的路由表，确认 R2 路由器已经学习其它区域的路由。

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C       172.16.255.0/30 is directly connected, Serial1/1
O IA    172.16.255.4/30 [110/128] via 172.16.255.2, 00:08:40, Serial1/1
O IA    172.16.255.8/30 [110/192] via 172.16.255.2, 00:06:20, Serial1/1
O IA    172.16.16.1/32 [110/193] via 172.16.255.2, 00:06:20, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
R1#
```

批注 [stanley164]: R1 路由器已经正确的学习到其它区域的路由。

10、使用 ping 命令确认路由有效性：

```
R1#ping 172.16.16.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.16.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/251/312 ms
R1#
```

11、实验完成。

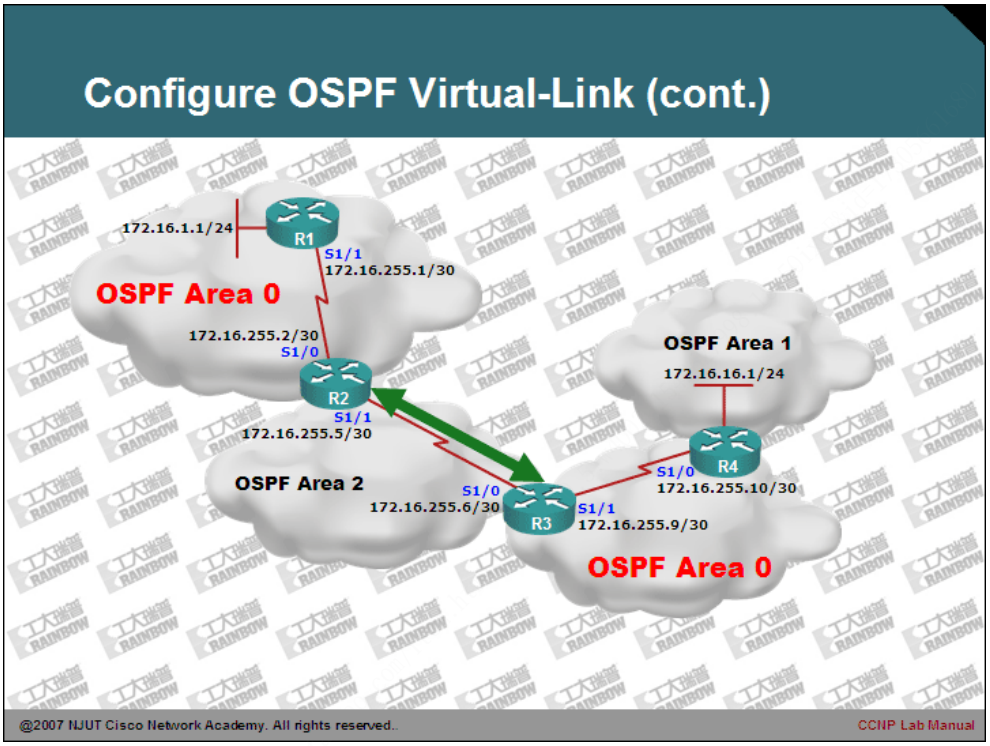
Lab 16. Configuring OSPF Virtual-Link（Cont.）

实验目的：

1、理解 OSPF 虚链路原理及何时需要使用虚链路。

2、掌握 OSPF 虚链路配置方法

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、首先配置 R2,R3,R4 的 OSPF 协议，配置过程中注意区域号：

3、完成配置后，查看 R1 的路由表。

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
O IA    172.16.255.4/30 [110/128] via 172.16.255.2, 00:02:11, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
R1#
```

批注 [stanley165]: R1 仅学习到 area 2 的路由。

4、查看 R2 的路由表：

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/0
C       172.16.255.4/30 is directly connected, Serial1/1
O       172.16.1.1/32 [110/65] via 172.16.255.1, 00:05:10, Serial1/0
R2#
```

批注 [stanley166]: R2 仅学习到 R1 所在 area 0 的路由

5、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.4/30 is directly connected, Serial1/0
C       172.16.255.8/30 is directly connected, Serial1/1
O IA    172.16.16.1/32 [110/65] via 172.16.255.10, 00:05:16, Serial1/1
R3#
```

批注 [stanley167]: R3 仅仅学习到 area 1 区域的路由。

6、查看 R4 路由表：

```
R4#show ip route

Gateway of last resort is not set
```

```
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O IA     172.16.255.4/30 [110/128] via 172.16.255.9, 00:19:32, Serial1/0
C        172.16.255.8/30 is directly connected, Serial1/0
C        172.16.16.0/24 is directly connected, Loopback0
R4#
```

批注 [stanley168]：r4 路由器仅学习到 area 2 的路由。

7、通过以上查看，可以发现，任何一台路由器都无法学习到完整的网络路由。

产生此问题的主要原因是：骨干 0 的区域被 area 2 分割，造成整个网络变成两个 OSPF 的自治系统。所以相互之间都无法学习完整的路由。

8、在这种情况下，可以通过配置虚链路来解决骨干被分割的问题。在 R2 与 R3 的路由器上实施如下配置：

```
R2(config)#router ospf 1
R2(config-router)#area 2 virtual-link 172.16.255.9
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley169]：创建虚链路。

命令中的 area 2 指出有一条虚链路存在于区域 2 中。virtual-link 172.16.255.9 指出创建虚链路的**对端 R3 路由器的 router id。**

```
R3(config)#router ospf 1
R3(config-router)#area 2 virtual-link 172.16.255.5
R3(config-router)#exit
R3(config)#exit
R3#
```

批注 [stanley170]：配置到 R2 路由器虚链路。
注意：使用 router id，而不是接口 ip.

9、查看任意一台路由，确认路由学习情况。本处选择 R1 路由器。

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C       172.16.255.0/30 is directly connected, Serial1/1
O IA    172.16.255.4/30 [110/128] via 172.16.255.2, 00:01:08, Serial1/1
O       172.16.255.8/30 [110/192] via 172.16.255.2, 00:01:08, Serial1/1
O IA    172.16.16.1/32 [110/193] via 172.16.255.2, 00:01:08, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
R1#
```

批注 [stanley171]：此时，R1 已经学习到完整的网络路由。

10、接下来，使用 ping 命令，确认路由是否有效。

```
R1#ping 172.16.16.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.16.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 188/239/288 ms
```

```
R1#
R1#
R1#ping 172.16.255.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.255.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/168/192 ms
R1#
```

11、此时，无法学习完整的路由问题已经被解决。OSPF Virtual Link 不仅可以解决普通区域与骨干区域非直接问题，还可以解决骨干被分割问题。但是，此类问题一般都是由于网络迁移或是本身设计问题所造成的。**OSPF 的虚链路仅仅是一种网络过渡的解决方案。**

12、实验完成。

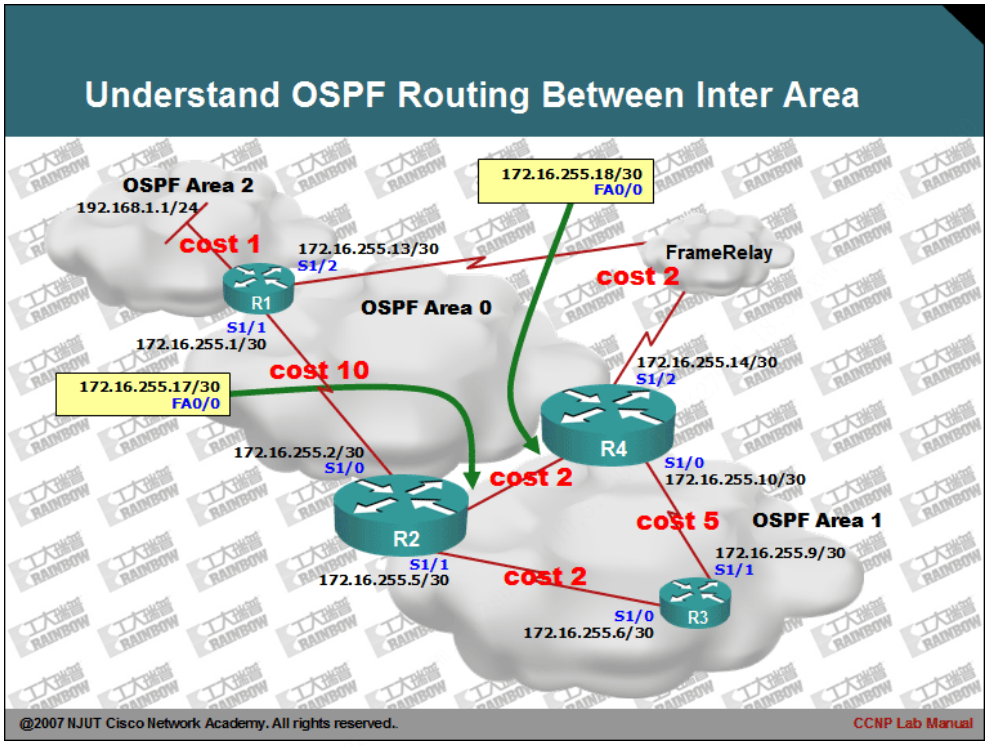
CCNP Lab Manual

Lab 17. Understand OSPF Routing Between Inter Area

实验目的：

1、理解 OSPF 内部区域间路由计算方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、R1 和 R4 路由，需要接口的网络类型，以便于 OSPF 能够自动创建邻居关系。

```
R1(config)#interface serial 1/2
R1(config-if)#ip ospf network broadcast
```

批注 [stanley172]：指定接口的 OSPF 的网络类型，确保 OSPF 能够自动的在 NBMA 的网络中创建邻居关系。

替代配置方法：在 OSPF 配置中使用 neighbor 命令手工配置邻居关系。

```
R4(config)#interface serial 1/2
R4(config-if)#ip ospf network broadcast
```

3、按拓扑规定，配置相应接口的 OSPF 的链路开销值(cost)。配置如下所示：

```
R3(config)#interface serial 1/0
R3(config-if)#ip ospf cost 2
R3(config-if)#exit
R3(config)#interface serial 1/1
R3(config-if)#ip ospf cost 5
R3(config-if)#exit
```

批注 [stanley173]：配置 OSPF 接口的 cost 值，此值影响外出的路由的度量计算。

即 R3 到达 R2 的 cost 值为 2。但不会影响 R2 到 R3 的 cost 的值的计算。

4、完成配置后。暂时不查看 R3 的路由表，分析一下 R3 到达 R1 的 192.168.1.0/24 网络路由。**OSPF 使用 cost 值来计算到达目标网络度量。当出现多条冗余的链路时，会使用 SPF 算法进行最佳路由计算与选择最佳路由。**本例中，R3 到达 192.168.1.0/24 的网络，共有如下几条路由可供选择：

编号	路径	COST 值
1#	R3 ------> R2 ------> R1 ------> 目标网络	13
2#	R3 ------> R2 ------> R4 ------> R1 ------> 目标网络	7
3#	R3 ------> R4 ------> R1 ------> 目标网络	8
4#	R3 ------> R4 ------> R2 ------> R1 ------> 目标网络	18

根据上述表格，所列出的各条路由来看，R3 路由器会先优先选择 2#路由，因为 2#路由的 cost 最小。为了确认猜测。查看 R3 的路由表：

```
R3#show ip route
.....
C       172.16.255.8 is directly connected, Serial1/1
O IA    172.16.255.12 [110/6] via 172.16.255.5, 00:04:01, Serial1/0
O       172.16.255.16 [110/4] via 172.16.255.5, 00:04:01, Serial1/0
O IA 192.168.1.0/24 [110/7] via 172.16.255.5, 00:04:01, Serial1/0
.....
R3#
```

批注 [stanley174]：R3 到达目标网络的所选择路由的 cost 值为 7。

路由表显示选择的是 2#路由。

使用 ping 确认路由有效性：

```
R3#ping 192.168.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/137/144 ms
R3#
```

批注 [stanley175]：路由是可用的。

为了确认确实使用了 2#路由，使用 traceroute 命令再次确认：

```
R3#traceroute 192.168.1.1

Type escape sequence to abort.
Tracing the route to 192.168.1.1

  1 172.16.255.5 52 msec 96 msec 96 msec
  2 172.16.255.1 144 msec *  168 msec
R3#
```

批注 [stanley176]：下一跳为 R2 路由器。

批注 [stanley177]：再一跳则到达了 R1 路由器。并没有按 2#路由器所述的转发给 R4 路由器。

5、产生这个问题的主要原因是：

当 R3 路由器在选择到达 R1 的 192.168.1.0/24 网络的路由时，使用得确实是 SPF 的算法。计算最短最佳路由。因此 R3 在比较几条路由器时，会选择从 R2,R4,R1 这样的路由，因为其 cost 值是 7。

当 R3 向数据包转发给 R2 的时候，R2 发现此数据包是要到达其它网络。**因此 R2 不会将数据包再转发给其相同区域的其它路由器。**因为 R2 自己是 ABR，他认为**到达其它区域的数据包，需要直接转发给骨干区域**。而自己也恰巧与骨干区域相连。因此 R2 直接将数据包转发给骨干区域的 R1 路由器。

正是因为这个原因，所以我们查看的路由跟实际转发数据包的路径不一致。

6、实验总结：

OSPF 区域间的路由，并不是完全根据 cost 值计算的最短路径优先算法。而是有点类似于距离矢量的算法。

7、实验完成。

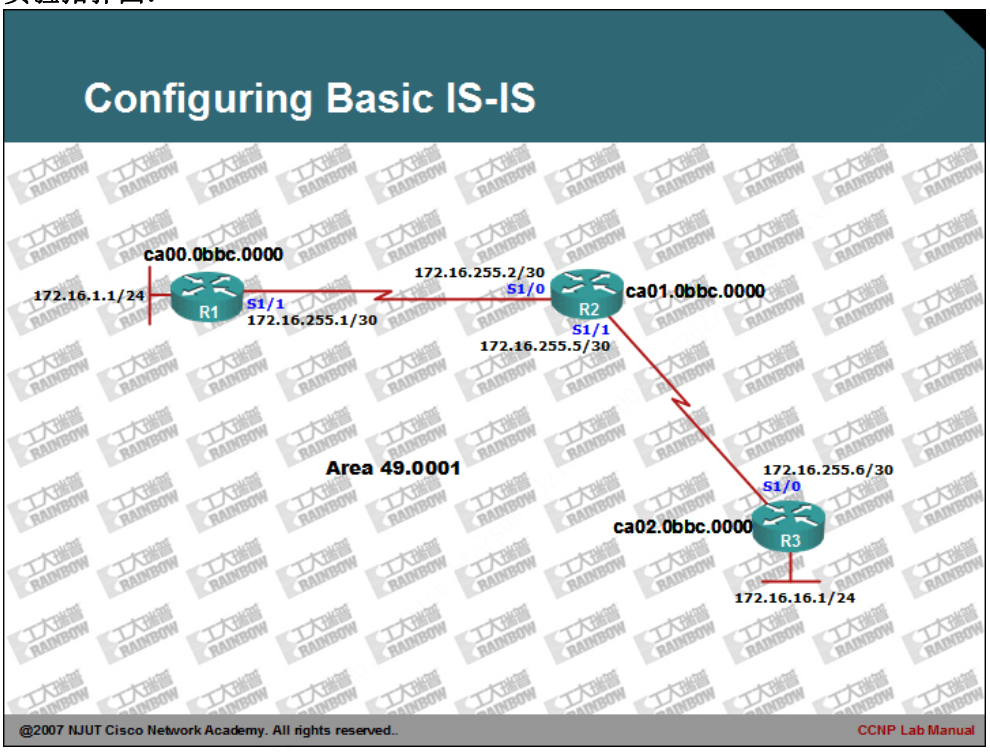
CCNP Lab Manual

Lab 18. Configuring Basic IS-IS

实验目的：

1、掌握基本的 IS-IS 路由协议配置。
2、理解 L1 类型路由。
3、掌握更改路由器的类型配置方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、在 R1、R2 和 R3 上启用 IS-IS 路由协议,具体配置如下。

```
R1(config)#router isis cisco
R1(config-router)#net 49.0001.ca00.0bbc.0000.00
R1(config-router)#exit
R1(config)#
R1(config)#interface loopback 0
R1(config-if)#ip router isis cisco
R1(config-if)#exit
R1(config)#interface serial 1/1
R1(config-if)#ip router isis cisco
R1(config-if)#exit
R1(config)#
```

批注 [stanley178]：启用 IS-IS 的路由进程。

cisco 标记类似 OSPF 进程号。

批注 [stanley179]：配置 R1 路由器的 NET 的地址。每个 NET 的系统 ID 都是由接口的 MAC 地址构成。

49.0001 为 area ID

ca00.0bbc.0000 为 R1 路由器的 system ID。在一个路由选择域内这个 ID 必须是唯一的。

00 为 R1 的 SEL,始终置为 00。用于描述与网络层的服务项相关联。

```
R2(config)#router isis cisco
R2(config-router)#net 49.0001.ca01.0bbc.0000.00
R2(config-router)#exit
R2(config)#interface serial 1/0
R2(config-if)#ip router isis cisco
R2(config-if)#exit
R2(config)#interface serial 1/1
R2(config-if)#ip router isis cisco
R2(config-if)#exit
R2(config)#exit
```

```
R3(config)#router isis cisco
R3(config-router)#net 49.0001.ca02.0bbc.0000.00
R3(config-router)#exit
R3(config)#interface serial 1/0
R3(config-if)#ip router isis cisco
R3(config-if)#exit
R3(config)#interface loopback 0
R3(config-if)#ip router isis cisco
R3(config-if)#exit
R3(config)#exit
```

批注 [stanley180]：在接口下启用 IS-IS 进程。
其类似于 RIP 或是 OSPF 在路由配置模式下的 network 命令的作用。

3、配置完成后，查看任一路由器的路由表：

```
R1#show ip route

Gateway of last resort is not set
```

```
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
i L1    172.16.255.4/30 [115/20] via 172.16.255.2, Serial1/1
i L1    172.16.16.0/24 [115/30] via 172.16.255.2, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
R1#
```

批注 [stanley181]: R1 从 R2 学习的 ISIS 的路由。

L1 的路由用描述相同区域的路由。

4、使用 ping 命令确认路由：

```
R1#ping 172.16.16.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.16.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/152/192 ms
R1#
```

5、查看 R2 路由器 ISIS 的邻居表：

```
R2#show isis neighbors
System Id      Type Interface IP Address      State Holdtime Circuit Id
R3               L1L2 Se1/1     172.16.255.6    UP    27       00
R1               L1L2 Se1/0     172.16.255.1    UP    28       00
R2#
R2#show clns neighbors
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R3             Se1/1       *HDLC*          Up     25        L1L2 IS-IS
R1             Se1/0       *HDLC*          Up     29        L1L2 IS-IS
R2#
```

批注 [stanley182]: Cisco 路由器默认是 L1/L2 的路由器类型。

批注 [stanley183]: 查看 clns 的邻居路由器。

6、查看主机名与系统标识符（system ID）。

```
R1#show isis hostname
Level  System ID      Dynamic Hostname  (cisco)
  1    CA01.0BBC.0000 R2
     * CA00.0BBC.0000 R1
  1    CA02.0BBC.0000 R3
R1#
```

批注 [stanley184]: 类似于 ARP 协议的映射。
其使用类型 137 的 TLV 动态交换获得的。
带有*号为当前路由器。

7、查看 IS-IS 的链路状态数据库，**由于默认情况下 CISCO 路由器即是 L1 又是 L2 的路由器。每一台路由器都会建立 L1 类型的邻接关系和 L2 类型的邻接关系。正是因为如此，每一台路由也会同时显示 L1 和 L2 类型的链路状态数据库。**

```
R1#show isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
```

```
01CA.000B.BC00.00-00   0x00000001   0x6107        0 (1083)          0/0/0
R1.00-00             * 0x00000005   0xDC1C        897               0/0/0
R2.00-00               0x00000005   0x21A8        787               0/0/0
R3.00-00               0x00000004   0xE2F0        717               0/0/0
IS-IS Level-2 Link State Database:
LSPID                  LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
01CA.000B.BC00.00-00   0x00000001   0x6107        0 (1083)          0/0/0
R1.00-00             * 0x00000007   0xD846        947               0/0/0
R2.00-00               0x00000007   0xF207        802               0/0/0
R3.00-00               0x00000005   0x7796        756               0/0/0
R1#
```

8、查看详细的链路状态数据库。

```
R1#show isis database detail

IS-IS Level-1 Link State Database:
LSPID                  LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00             * 0x00000008   0xD61F        924               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname: R1
  IP Address:   172.16.1.1
  Metric: 10         IP 172.16.255.0 255.255.255.252
  Metric: 10         IP 172.16.1.0 255.255.255.0
  Metric: 10         IS R2.00
R2.00-00               0x00000008   0x1BAB        897               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname: R2
  IP Address:   172.16.255.5
.................
R3.00-00               0x00000008   0x7199        754               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname: R3
  IP Address:   172.16.16.1
  Metric: 10         IS R2.00
  Metric: 20         IP 172.16.255.0 255.255.255.252
  Metric: 10         IP 172.16.255.4 255.255.255.252
  Metric: 10         IP 172.16.16.0 255.255.255.0
  Metric: 30         IP 172.16.1.0 255.255.255.0
```

批注 [stanley185]：区域 ID

批注 [stanley186]：默认情况下，IS-IS 认为到达直连网络的度量是 10.

批注 [stanley187]：到达目标网的度量显示。

9、在小型网络中，路由器保留他们的缺省的路由器类型配置是可以接受的。当网络较大的时候，使用缺省类型，将会降低路由器的效率。因为这需要同时维

护两张链路状态数据库表。会消耗大量的 CPU 和内存的资源。因此可以给不同路由器手工指定合适的类型。

在本实验中，因为没有多区域的存在，所以可以将所有的路由器指定 Level-1 的路由器类型。

在 R1、R2 和 R3 的路由器手工配置路由器的类型：

```
R1(config)#router isis cisco
R1(config-router)#is-type level-1
R1(config-router)#exit
R1(config)#exit
```

批注 [stanley188]：指定路由器类型为 Level-1 路由器。

这样可以有效避免需要同时维护两张表。增加了协议工作效率。

```
R2(config)#router isis cisco
R2(config-router)#is-type level-1
R2(config-router)#exit
R2(config)#exit
```

```
R3(config)#router isis cisco
R3(config-router)#is-type level-1
R3(config-router)#exit
```

10、再次查看 R1 的链路状态数据库，确认更改：

```
R1#show isis database
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x0000000A   0xD025        829               0/0/0
R2.00-00              0x0000000B   0x13B2        835               0/0/0
R3.00-00              0x00000009   0xD6F9        834               0/0/0
R1#
```

批注 [stanley189]：此时，链路状态数据库中仅有 L1 的类型的数据存在。

11、实验完成.

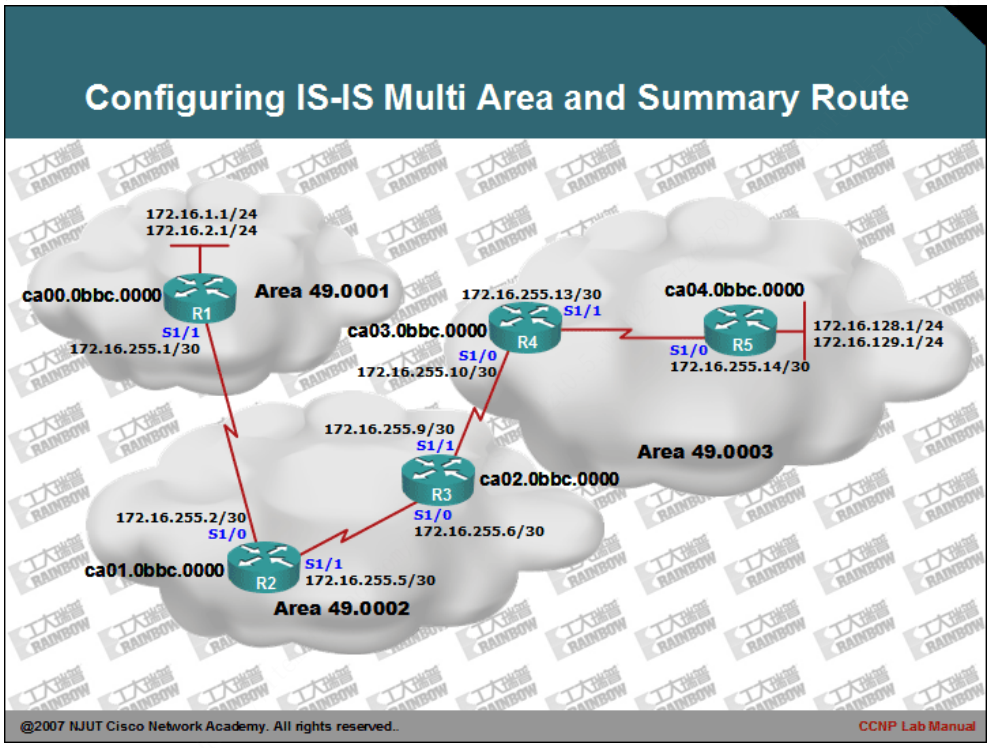
CCNP Lab Manual

Lab 19. Configuring IS-IS Multi Area and Summary Route

实验目的：

1、掌握基本的 IS-IS 路由协议配置。
2、理解 L1/L2 类型路由。
3、掌握 IS-IS 区域汇总的配置。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、各台路由器的 IS-IS 配置如下。

```
R1(config)#interface Loopback0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip router isis cisco
R1(config-if)#isis circuit-type level-1
R1(config-if)#exit
R1(config)#
R1(config)#interface Loopback1
R1(config-if)#ip address 172.16.2.1 255.255.255.0
R1(config-if)#ip router isis cisco
R1(config-if)#isis circuit-type level-1
R1(config-if)#exit
R1(config)#
R1(config)#interface Serial1/1
R1(config-if)#ip address 172.16.255.1 255.255.255.252
R1(config-if)#ip router isis cisco
R1(config-if)#isis circuit-type level-2-only
R1(config-if)#exit
R1(config)#
R1(config)#router isis cisco
R1(config-if)#net 49.0001.ca00.0bbc.0000.00
R1(config-if)#exit
R1(config)#
```

批注 [stanley190]：指定此接口发送 level-1 的路由报文。

默认情况下：IS-IS 的 Level-1-2 的路由器，会向所有接口中发送 Level-1 和 Level-2 的报文。通过此条命令可以修剪掉不必要的报文发送。

批注 [stanley191]：指定 s1/1 发送 level-2 的报文

```
R2(config)#interface Serial1/0
R2(config-if)#ip address 172.16.255.2 255.255.255.252
R2(config-if)#ip router isis cisco
R2(config-if)#isis circuit-type level-2-only
R2(config-if)#exit
R2(config)#
R2(config)#interface Serial1/1
R2(config-if)#ip address 172.16.255.5 255.255.255.252
R2(config-if)#ip router isis cisco
R2(config-if)#exit
R2(config)#
R2(config)#router isis cisco
R2(config-if)#net 49.0002.ca01.0bbc.0000.00
R2(config-if)#exit
R2(config)#
```

批注 [stanley192]：指定 s1/0 接口发送 level-2 报文

```
R3(config)#interface Serial1/0
R3(config-if)#ip address 172.16.255.6 255.255.255.252
R3(config-if)#ip router isis cisco
R3(config-if)#exit
R3(config)#
R3(config-if)#interface Serial1/1
R3(config-if)#ip address 172.16.255.9 255.255.255.252
R3(config-if)#ip router isis cisco
R3(config-if)#isis circuit-type level-2-only
R3(config-if)#exit
R3(config)#
R3(config-if)#router isis cisco
R3(config-if)#net 49.0002.ca02.0bbc.0000.00
R3(config-if)#exit
R3(config)#
```

批注 [stanley193]: 指定此接口仅发送 level-2 报文

```
R4(config)#interface Serial1/0
R4(config-if)#ip address 172.16.255.10 255.255.255.252
R4(config-if)#ip router isis cisco
R4(config-if)#isis circuit-type level-2-only
R4(config-if)#exit
R4(config)#
R4(config-if)#interface Serial1/1
R4(config-if)#ip address 172.16.255.13 255.255.255.252
R4(config-if)#ip router isis cisco
R4(config-if)#isis circuit-type level-1
R4(config-if)#exit
R4(config)#
R4(config-if)#router isis cisco
R4(config-if)#net 49.0003.ca03.0bbc.0000.00
R4(config)#exit
R4(config)#
```

```
R5(config)#interface Loopback0
R5(config-if)#ip address 172.16.128.1 255.255.255.0
R5(config-if)#ip router isis cisco
R5(config-if)#isis circuit-type level-1
R5(config-if)#exit
R5(config)#
R5(config-if)#interface Loopback1
R5(config-if)#ip address 172.16.129.1 255.255.255.0
R5(config-if)#ip router isis cisco
R5(config-if)#exit
```

批注 [stanley194]: 如果路由器被指定为 level-1，则此条命令可以被省略。

```
R5(config)#
R5(config-if)#interface Serial1/0
R5(config-if)#ip address 172.16.255.14 255.255.255.252
R5(config-if)#ip router isis cisco
R5(config-if)#exit
R5(config)#
R5(config-if)#router isis cisco
R5(config-if)#net 49.0003.ca04.0bbc.0000.00
R5(config-if)#is-type level-1
R5(config-if)#exit
R5(config)#
```

批注 [stanley195]：指定路由器为 level-1 类型路由器。

4、查看 R2、R3、R4 的邻居表，观察其多区域环境下的邻居关系：

```
R2#show isis neighbors
System Id      Type Interface IP Address      State Holdtime Circuit Id
R3             L1L2 Se1/1     172.16.255.6    UP    29       01
R1             L2   Se1/0     172.16.255.1    UP    23       00
R2#
```

批注 [stanley196]：与 R1 创建 L1/L2 类型邻居。

批注 [stanley197]：与 R3 创建 L2 类型邻居。

```
R3#show isis neighbors
System Id      Type Interface IP Address      State Holdtime Circuit Id
R2             L1L2 Se1/0     172.16.255.5    UP    25       01
R4             L2   Se1/1     172.16.255.10   UP    27       00
R3#
```

```
R4#show isis neighbors
System Id      Type Interface IP Address      State Holdtime Circuit Id
R3             L2   Se1/0     172.16.255.9    UP    23       00
R5             L1   Se1/1     172.16.255.14   UP    22       00
R4#
```

5、查看 R1 与 R5 的路由表，观察其区别：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
i L2    172.16.128.0/24 [115/50] via 172.16.255.2, Serial1/1
i L2    172.16.129.0/24 [115/50] via 172.16.255.2, Serial1/1
C       172.16.255.0/30 is directly connected, Serial1/1
i L2    172.16.255.4/30 [115/20] via 172.16.255.2, Serial1/1
i L2    172.16.255.8/30 [115/30] via 172.16.255.2, Serial1/1
i L2    172.16.255.12/30 [115/40] via 172.16.255.2, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
C       172.16.2.0/24 is directly connected, Loopback1
```

批注 [stanley198]：由于 R1 是 L1/L2 类型的路由器，所以 R1 能够学习到 L2 的其它区域的路。
同时，如果查看 R1 链路状态数据库。会发现 R1 同时维护了 L1 和 L2 的数据库。

```
R1#
```

```
R1#show isis database
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x0000000B   0xD33B        679               1/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x0000000E   0xCC4D        736               0/0/0
R2.00-00              0x00000013   0xA297        427               0/0/0
R3.00-00              0x0000000F   0x65C8        1097              0/0/0
R4.00-00              0x00000011   0x4B41        818               0/0/0
R1#
```

```
R5#show ip route

Gateway of last resort is 172.16.255.13 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.128.0/24 is directly connected, Loopback0
C       172.16.129.0/24 is directly connected, Loopback1
C       172.16.255.12/30 is directly connected, Serial1/0
i*L1 0.0.0.0/0 [115/10] via 172.16.255.13, Serial1/0
R5#
R5#show isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R4.00-00              0x0000000C   0x7BA1        770               1/0/0
R5.00-00            * 0x0000000D   0xF411        649               0/0/0
R5#
```

批注 [stanley199]：由于 R5 是 Level-1 的路由器，其处在 Area 49.0003 区域内部。因此其会接到 R4 路由器发送的 L1 类型的默认路由。

这样做的优点是：能够有效的减少路由表的大小，增强了 IS-IS 的稳定性。

其做法类似于 OSPF 的完全末节区域（Totally Stub）

批注 [stanley200]：R5 路由仅有 L1 的数据库。

6、使用 ping 命令确认路由：

```
R1#ping 172.16.129.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.129.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 220/240/264 ms
```

7、为了能够更有效的减小路由表的大小，还可以配置 IS-IS 的汇总。首先查看 R4 的路由表：

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
i L1    172.16.128.0/24 [115/20] via 172.16.255.14, Serial1/1
i L1    172.16.129.0/24 [115/20] via 172.16.255.14, Serial1/1
i L2    172.16.255.0/30 [115/30] via 172.16.255.9, Serial1/0
i L2    172.16.255.4/30 [115/20] via 172.16.255.9, Serial1/0
C       172.16.255.8/30 is directly connected, Serial1/0
C       172.16.255.12/30 is directly connected, Serial1/1
i L2    172.16.1.0/24 [115/40] via 172.16.255.9, Serial1/0
i L2    172.16.2.0/24 [115/40] via 172.16.255.9, Serial1/0
R4#
```

批注 [stanley201]：配置汇总对此路由进行总结。

8、在 R1 上配置地址总结：

```
R1(config)#router isis cisco
R1(config-router)#summary-address 172.16.0.0 255.255.128.0
R1(config-router)#exit
R1(config)#exit
```

批注 [stanley202]：对 R1 的两个直连回环口进行地址总结。

9、再次查看 R4 的路由表：

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
i L1    172.16.128.0/24 [115/20] via 172.16.255.14, Serial1/1
i L1    172.16.129.0/24 [115/20] via 172.16.255.14, Serial1/1
i L2    172.16.255.0/30 [115/30] via 172.16.255.9, Serial1/0
i L2    172.16.255.4/30 [115/20] via 172.16.255.9, Serial1/0
C       172.16.255.8/30 is directly connected, Serial1/0
C       172.16.255.12/30 is directly connected, Serial1/1
i L2    172.16.0.0/17 [115/40] via 172.16.255.9, Serial1/0
R4#
```

批注 [stanley203]：此条路由指出 R1 的 172.16.1.0/24 和 172.16.2.0/24 的网络被成功的汇总。

10、确认汇总路由有效性：

```
R4#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 192/225/240 ms
R4#
```

11、实验完成.

CCNP Lab Manual

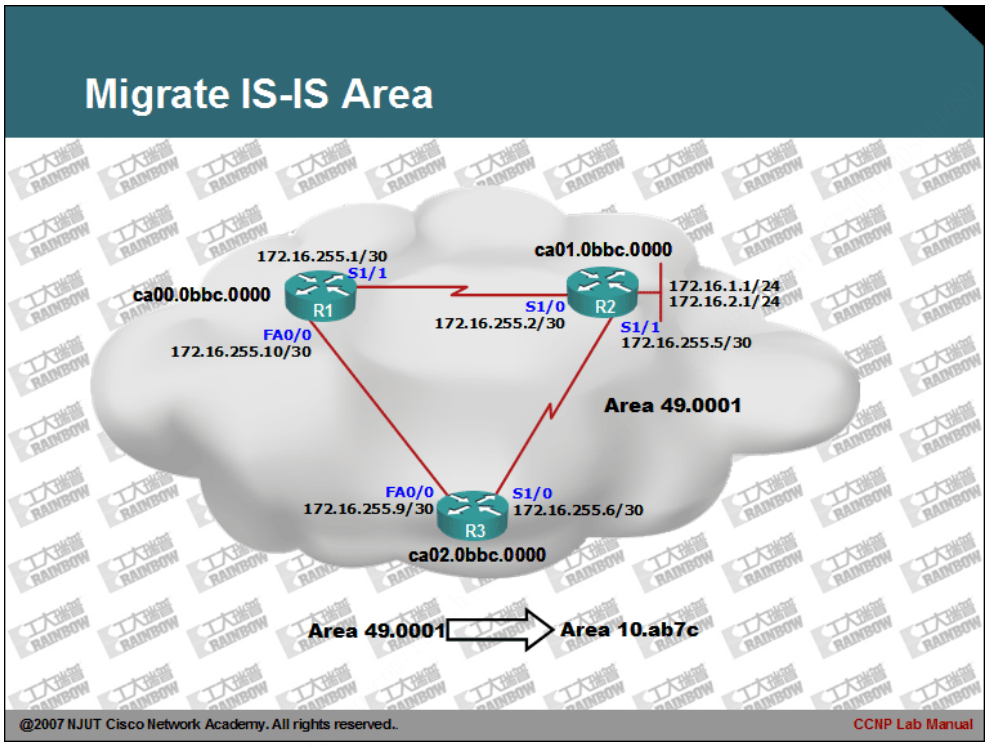
Lab 20. Migrate IS-IS Area

实验目的：

1、理解 IS-IS 区域迁移的原理。

2、掌握 IS-IS 的区域迁移配置。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置各台路由器的 IS-IS 协议。

3、查看 R1 的路由表：

```
R1#show ip route

Gateway of last resort is 172.16.255.2 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
i L1    172.16.255.4/30 [115/20] via 172.16.255.2, Serial1/1
                        [115/20] via 172.16.255.9, FastEthernet0/0
C       172.16.255.8/30 is directly connected, FastEthernet0/0
i L1    172.16.1.0/24 [115/20] via 172.16.255.2, Serial1/1
i L1    172.16.2.0/24 [115/20] via 172.16.255.2, Serial1/1
R1#R1#
```

4、查看任一路由器的链路状态数据库：

```
R1#show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x00000008   0x8D3B        1116              0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname: R1
  IP Address:   172.16.255.1
  Metric: 10         IP 172.16.255.8 255.255.255.252
  Metric: 10         IP 172.16.255.0 255.255.255.252
  Metric: 10         IS R3.01
  Metric: 10         IS R2.00
.....
R1#
```

批注 [stanley204]：当前的区域 ID 为:49.0001

5、配置区域向 10.abc7 迁移。在三台路由器原有的配置基础上作如下配置：

```
R1(config)#router isis cisco
R1(config-router)#net 10.abc7.ca00.0bbc.0000.00
R1(config)#exit
R1(config)#
```

批注 [stanley205]：配置第二个 NET 地址。

```
R2(config)#router isis cisco
R2(config-router)#net 10.abc7.ca01.0bbc.0000.00
R2(config)#exit
R2(config)#
```

```
R3(config)#router isis cisco
R3(config-router)#net 10.abc7.ca02.0bbc.0000.00
R3(config)#exit
R3(config)#
```

6、再次查看任意一台路由器的链路状态数据库：

```
R1#show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x00000009   0xAF8D        991               0/0/0
  Area Address: 49.0001
  Area Address: 10.abc7
  NLPID:        0xCC
  Hostname: R1
  IP Address:   172.16.255.1
  Metric: 10         IP 172.16.255.8 255.255.255.252
  Metric: 10         IP 172.16.255.0 255.255.255.252
  Metric: 10         IS R3.01
  Metric: 10         IS R2.00
.....
```

批注 [stanley206]：此时会发现在链路状态数据库中出现两个区域地址。

可以看出网络内的每一台路路器都是和多区域相连的。

7、查看任意一台路由器的 clns 的邻居表：

```
R1#show clns is-neighbors detail

System Id      Interface   State  Type Priority  Circuit Id         Format
R3             Fa0/0       Up     L1   64        R3.01              Phase V
  Area Address(es): 49.0001 10.abc7
  IP Address(es):  172.16.255.9*
  Uptime: 00:08:06
  NSF capable
R2             Se1/1       Up     L1   0         01                 Phase V
  Area Address(es): 49.0001 10.abc7
  IP Address(es):  172.16.255.2*
  Uptime: 00:08:18
  NSF capable
R1#
```

批注 [stanley207]：显示相同的两个区域号。

8、当确认每一台路由器都同时处于需要迁移的区域的区域号时，则可以删除原来的 NET 地址语句，配置如下：

```
R1(config)#router isis cisco
R1(config-router)#no net 49.0001.ca00.0bbc.0000.00
R1(config-router)#exit
R1(config)#
```

```
R2(config)#router isis cisco
R2(config-router)#no net 49.0001.ca01.0bbc.0000.00
R2(config-router)#exit
R2(config)#
```

```
R3(config)#router isis cisco
R3(config-router)#no net 49.0001.ca02.0bbc.0000.00
R3(config-router)#exit
R3(config)#
```

9、查看 R1 路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
i L1    172.16.255.4/30 [115/20] via 172.16.255.2, Serial1/1
                        [115/20] via 172.16.255.9, FastEthernet0/0
C       172.16.255.8/30 is directly connected, FastEthernet0/0
i L1    172.16.1.0/24 [115/20] via 172.16.255.2, Serial1/1
i L1    172.16.2.0/24 [115/20] via 172.16.255.2, Serial1/1
.....
```

10、查看 R1 的链路状态数据库：

```
R1#show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00            * 0x0000000F   0xEC9B        1065              0/0/0
  Area Address: 10.abc7
  NLPID:        0xCC
  Hostname: R1
  IP Address:   172.16.255.1
  Metric: 10         IP 172.16.255.8 255.255.255.252
  Metric: 10         IP 172.16.255.0 255.255.255.252
  Metric: 10         IS R2.00
  Metric: 10         IS R3.01
.....
```

批注 [stanley208]：显示为迁移后的区域。

11、迁移成功，实验完成。

CCNP Lab Manual

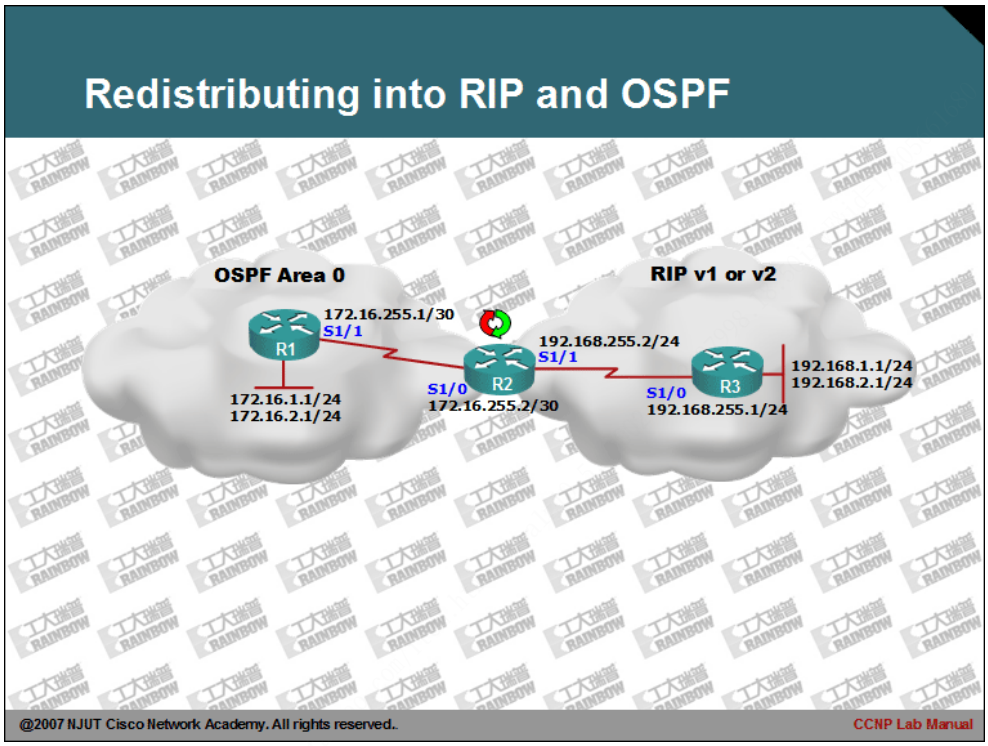
Lab 21. Redistributing into RIP and OSPF

实验目的：

1、掌握 RIP 与 OSPF 的重发布配置。

2、理解 OSPF 的 E1 与 E2 类型的路由。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 R1 与 R2 的 OSPF 路由协议和 R2 与 R3 的 RIP 路由协议。

3、查看 R1、R2 和 R3 的路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
C       172.16.2.0/24 is directly connected, Loopback1
R1#
```

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/0
O       172.16.1.0/24 [110/65] via 172.16.255.1, 00:02:47, Serial1/0
O       172.16.2.0/24 [110/65] via 172.16.255.1, 00:02:47, Serial1/0
     192.168.255.0/30 is subnetted, 1 subnets
C       192.168.255.0 is directly connected, Serial1/1
R    192.168.1.0/24 [120/1] via 192.168.255.1, 00:00:10, Serial1/1
R    192.168.2.0/24 [120/1] via 192.168.255.1, 00:00:10, Serial1/1
R2#
```

批注 [stanley209]： 从 R1 学习到的 OSPF 网络路由

批注 [stanley210]： 从 R3 学习到的 RIP 网络路由

```
R3#show ip route

Gateway of last resort is not set

C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback1
R3#
```

4、根据 show ip route 命令可以看出，只有 R2 路由才可以学习到整个网络的完整路由。是因为，R2 路由处于 OSPF 与 RIP 网络的边界。其同时运行了两种不同的路由协议。

5、为了确保 R1 和 R2 能够学习到整个网络路由。在 R2 上配置路由重发布。配置如下：

```
R2(config)#router ospf 1
R2(config-router)#redistribute rip metric 200 subnets
R2(config-router)#exit
R2(config)#router rip
R2(config-router)#redistribute ospf 1 metric 10
R2(config-router)#exit
```

6、查看 R1 路由器和 R3 路由器的路由表：

```
R1#show ip router
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
C       172.16.2.0/24 is directly connected, Loopback1
     192.168.255.0/30 is subnetted, 1 subnets
O E2    192.168.255.0 [110/200] via 172.16.255.2, 00:02:47, Serial1/1
O E2 192.168.1.0/24 [110/200] via 172.16.255.2, 00:02:53, Serial1/1
O E2 192.168.2.0/24 [110/200] via 172.16.255.2, 00:02:53, Serial1/1
R1#
```

```
R3#show ip router
R    172.16.0.0/16 [120/10] via 192.168.255.2, 00:00:24, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback1
R3#
```

7、确认路由有效性：

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/137/144 ms
R1#
```

```
R3#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/148/192 ms
```

批注 [stanley211]： 将 rip 网络的路由重发布到 OSPF 的网络中。并且指定其度量为 200

Subnets 命令可以确保 RIP 网络中的无类子网路由能够正确的被发布。

重发布的路由默认类型为 E2 类型。

关于 E1 与 E2 的路由详解，请查阅 OSPF 的区域总结部分实验。

批注 [stanley212]： 将 OSPF 网络路由重发布到 RIP 中。并指定其度量跳数为：10。

批注 [stanley213]： R1 已经通过重发布的配置，学习到了 RIP 网络的路由。

批注 [stanley214]： R3 学习到的 OSPF 的路由。

由于 R2 处于主类的边界。所以此处学习到的是汇总路由。

```
R3#
```

8、实验完成。

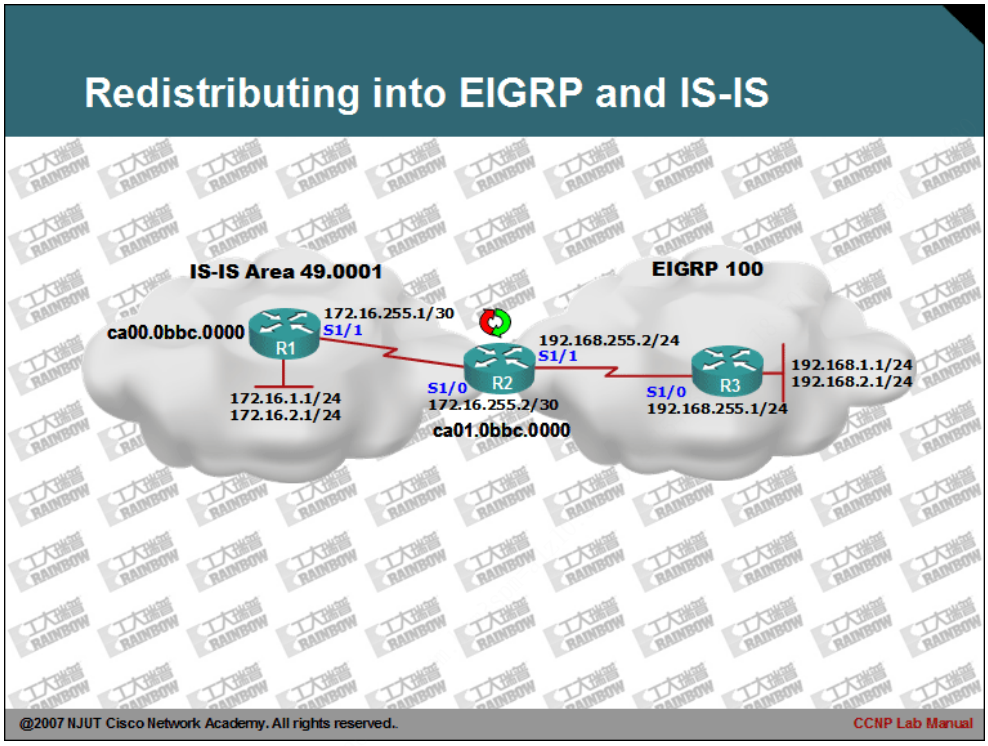
CCNP Lab Manual

Lab 22. Redistributing into EIGRP and IS-IS

实验目的：

1、掌握 EIGRP 与 IS-IS 的重发布配置。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 R1 与 R2 的 IS-IS 路由协议和 R2 与 R3 的 EIGRP 路由协议。

3、查看 R1、R2 和 R3 的路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
C       172.16.2.0/24 is directly connected, Loopback1
R1#
```

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/0
i L1    172.16.1.0/24 [115/20] via 172.16.255.1, Serial1/0
i L1    172.16.2.0/24 [115/20] via 172.16.255.1, Serial1/0
     192.168.255.0/30 is subnetted, 1 subnets
C       192.168.255.0 is directly connected, Serial1/1
D    192.168.1.0/24 [90/2297856] via 192.168.255.1, 00:00:04, Serial1/1
D    192.168.2.0/24 [90/2297856] via 192.168.255.1, 00:00:04, Serial1/1
R2#
```

批注 [stanley215]： 通过 IS-IS 学习到的 L1 的路由。

批注 [stanley216]： 通过 EIGRP 学习到的 R3 路由

```
R3#show ip route

Gateway of last resort is not set

C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback1
R3#
*Mar 29 10:39:29.171: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

4、根据 show ip route 命令可以看出，只有 R2 路由才可以学习到整个网络的完

整路由。是因为，R2 路由处于 EIGRP 与 IS-IS 网络的边界。其同时运行了两种不同的路由协议。

5、为了确保 R1 和 R2 能够学习到整个网络路由。在 R2 上配置路由重发布。配置如下：

```
R2(config)#router isis cisco
R2(config-router)#redistribute eigrp 100 metric 20 level-2
R2(config-router)#exit
R2(config)#
R2(config)#router eigrp 100
R2(config)#redistribute isis cisco level-1-2 metric 100000 10 255 1 1500
R2(config)#
```

因为 EIGRP 采用的是复合型的度量值，所以在重发布时，需要根据网络的实际情况指定相应的度量值。

6、查看 R1 路由器和 R3 路由器的路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.255.0/30 is directly connected, Serial1/1
C       172.16.1.0/24 is directly connected, Loopback0
C       172.16.2.0/24 is directly connected, Loopback1
     192.168.255.0/30 is subnetted, 1 subnets
i L2    192.168.255.0 [115/30] via 172.16.255.2, Serial1/1
i L2 192.168.1.0/24 [115/30] via 172.16.255.2, Serial1/1
i L2 192.168.2.0/24 [115/30] via 172.16.255.2, Serial1/1
R1#
```

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
D EX    172.16.1.0 [170/2172416] via 192.168.255.2, 00:08:48, Serial1/0
D EX    172.16.2.0 [170/2172416] via 192.168.255.2, 00:08:48, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback1
R3#
```

7、确认路由有效性：

批注 [stanley217]： 将本地的 EIGRP 路由协议学习到的路由重发布到 IS-IS 的网络。
并指定度量是 20
Level-2 是指出重发布的路由类型为 L2 的路由。

注：还可以追加 metric-type extenal 子参数，同时计算外部度量。

批注 [stanley218]： 将本址的 IS-IS 的路由协议学习到的路由重发布到 EIGRP 100 的网络中。
Level-1-2 指出需要重发布的路由为 L1 和 L2。
Metric 后的几个数值分别表示：
100000 ： 带宽值 100mbps
10 ： 网络延迟
255 ： 可靠度 100%
1 ： 负载 1%
1500 ： MTU 值。

批注 [stanley219]： 通过重发布学习到的路由。

其 metric 值为 30，这是因为，R1 在学习外部路由时，还计算本地到达 R2 路由器的度量值。

IS-IS 默认接口的度量为:10

批注 [stanley220]： 通过重发布学习到的 IS-IS 路由。EX 关键字，指出此路由为非 EIGRP 自治系统路由。

```
R3#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/94/96 ms
R3#
```

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

批注 [stanley221]：从 R1 上去 ping 路由器 R3 的回环口。
5 个数据包全部丢失。

8、再次查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
D EX    172.16.1.0 [170/2172416] via 192.168.255.2, 00:23:06, Serial1/0
D EX    172.16.2.0 [170/2172416] via 192.168.255.2, 00:23:06, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopbac
R3#
```

批注 [stanley222]：仅有 IS-IS 网络的两个路由。

查看路由发现缺少 172.16.255.0/24 网络路由。产生此问题的原因是：IS-IS 在重发布时，不会将直连网段重发布。

9、在 R2 上 EIGRP 协议中添加配置重发布直连网络：

```
R2(config)#router eigrp 100
R2(config-router)#redistribute connected metric 100000 10 255 1 1500
R2(config-router)#exit
```

批注 [stanley223]：将 R2 的直连网络重发布到 EIGPR 网络中。

10、查看 R3 路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D EX    172.16.255.0/30 [170/2172416] via 192.168.255.2, 00:00:06, Serial1/0
```

批注 [stanley224]：此时，r3 正确学习到的 r2 与 r1 的直连网络路由。

```
D EX    172.16.1.0/24 [170/2172416] via 192.168.255.2, 00:26:56, Serial1/0
D EX    172.16.2.0/24 [170/2172416] via 192.168.255.2, 00:26:56, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback1
R3#
```

11、在 R3 上确认路由有效性：

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/148/168 ms
R1#
```

批注 [stanley225]：此时网络已经可以正常访问。

12、实验完成。

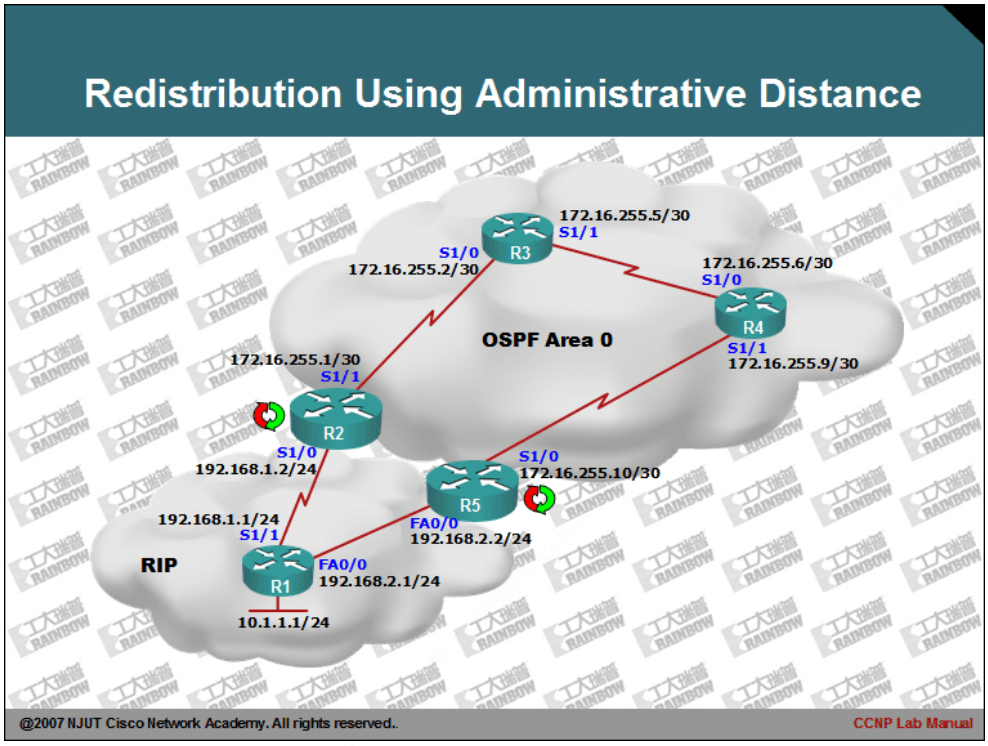
CCNP Lab Manual

Lab 23. Redistribution Using Administrative Distance

实验目的：

1、掌握通过修改管理距离解决重发布选择次佳路由问题。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、按照拓扑配置 RIP 和 OSPF 的路由协议。

3、查看 R2 和 R5 的路由表：

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.255.0 is directly connected, Serial1/1
O       172.16.255.4 [110/128] via 172.16.255.2, 00:01:44, Serial1/1
O       172.16.255.8 [110/192] via 172.16.255.2, 00:01:44, Serial1/1
R    10.0.0.0/8 [120/1] via 192.168.1.1, 00:00:21, Serial1/0
C    192.168.1.0/24 is directly connected, Serial1/0
O E2 192.168.2.0/24 [110/200] via 172.16.255.2, 00:01:44, Serial1/1
R2#
```

```
R5#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
O       172.16.255.0 [110/192] via 172.16.255.9, 00:02:08, Serial1/0
O       172.16.255.4 [110/128] via 172.16.255.9, 00:02:08, Serial1/0
C       172.16.255.8 is directly connected, Serial1/0
O E2 10.0.0.0/8 [110/200] via 172.16.255.9, 00:02:08, Serial1/0
O E2 192.168.1.0/24 [110/200] via 172.16.255.9, 00:02:08, Serial1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R5#
```

批注 [stanley226]：到达 10.0.0.0/8 的网络通过 172.16.255.9 下一跳。

4、通过观察两台路由器的路表，可以看出 R5 路由器到达 10.0.0.0/8 的网络并不是直接通过 R1 路由器，而是通过 R4-->R3-->R2-->R1-->10.0.0.0/8。通过拓扑可以看出，此条路由并不是最佳的路由。产生此问题的最主要的原因是：因为在 R2 路由器上配置路由重发布，R2 将 10.0.0.0/8 网络通告给其它的路由器时，其重发布路由的管理距离是 110，即 OSPF 的管理距离。当此条路由到达 R5 上时，R5 会比较 RIP 与 OSPF 的管理距离后，再决定采用谁的路由。因此造成了 R5 认为到达 10.0.0.0/8 网络最佳路由是通过 OSPF 的区域。而不是直接选择从 R1 到

达。**是因为：管理距离决定路由器选择何种路由协议产生的路由。**

5、为了解决此问题，我们可以通过修改本地某条路由的管理距离来强制路由器选择最佳路由，配置如下：

```
R5(config)#access-list 1 permit 10.0.0.0 0.255.255.255
R5(config)#router rip
R5(config-router)#distance 80 192.168.2.1 0.0.0.0 1
R5(config-router)#exit
R5(config)#exit
```

批注 [stanley227]：使用 ACL 匹配需要变更管理距离的网络。

批注 [stanley228]：将从 192.168.1.2 路由器发送匹配 ACL 1 指定网络路由的管理距离修改为 80。

6、再次查看 R5 的路由表：

```
R5#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
O       172.16.255.0 [110/192] via 172.16.255.9, 00:00:02, Serial1/0
O       172.16.255.4 [110/128] via 172.16.255.9, 00:00:02, Serial1/0
C       172.16.255.8 is directly connected, Serial1/0
R    10.0.0.0/8 [80/1] via 192.168.2.1, 00:00:02, FastEthernet0/0
O E2 192.168.1.0/24 [110/200] via 172.16.255.9, 00:00:02, Serial1/0
C    192.168.2.0/24 is directly connected, FastEther
```

批注 [stanley229]：此时 10.0.0.0/8 网络路由的管理已经变为 80。因此路由优先选择了 RIP 协议产生的路由。

7、为了确保网络的稳定，因此建议在 R2 路由器上也采用相同的配置，进行管理距离值的设定。具体配置请参照第 6 步。

8、实验完成。

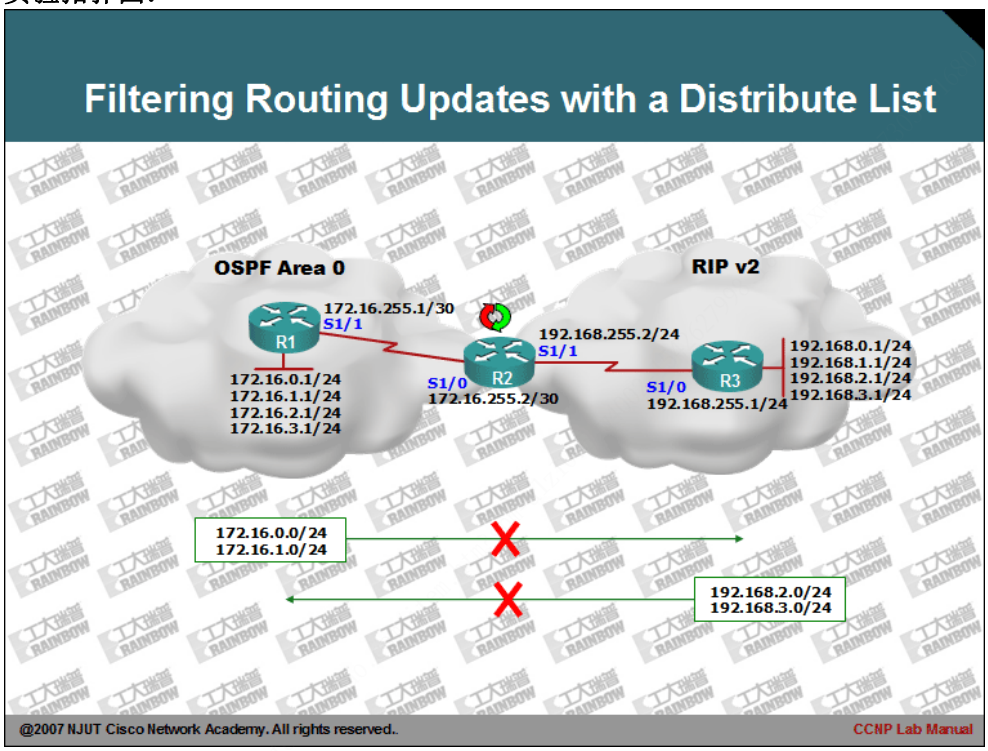
CCNP Lab Manual

Lab 24. Filtering Routing Updates with a Distribute List

实验目的：

1、掌握基于 distribute 命令的路由过滤配置方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、按照拓扑配置 OSPF 和 RIP v2 的路由协议。并关闭 RIP v2 的自动汇总。

3、在 R2 上配置路由重发布。

4、查看 R1 和 R3 的路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 5 subnets
C       172.16.255.0 is directly connected, Serial1/1
C       172.16.0.0 is directly connected, Loopback0
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback0
C       172.16.3.0 is directly connected, Loopback0
O E2 192.168.255.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.0.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.1.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.2.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.3.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
R1#
```

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 5 subnets
R       172.16.255.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.0.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.1.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.2.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.3.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.0.0/24 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback0
C    192.168.3.0/24 is directly connected, Loopback0
R3#
```

5、根据拓扑的需要，在 R2 上配置路由过滤，以过滤 OSPF 的路由。配置如下：

```
R2(config)#access-list 1 deny 172.16.0.0 0.0.0.255
R2(config)#access-list 1 deny 172.16.1.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#router rip
R2(config-router)#distribute-list 1 out ospf 1
R2(config-router)#exit
R2(config)#
```

批注 [stanley230]：首先配置 ACL，标识需要过滤的网络号。

批注 [stanley231]：在 RIP 协议下配置 distribute 列表，引用访问控制列表 1，过滤从 OSPF 重发布 RIP 的网络路由。

6、查看 R3 的路由，进行确认：

```
R3#show ip route

Gateway of last resort is not set

R       172.16.255.0 [120/10] via 192.168.255.2, 00:00:02, Serial1/0
R       172.16.2.0 [120/10] via 192.168.255.2, 00:00:02, Serial1/0
R       172.16.3.0 [120/10] via 192.168.255.2, 00:00:02, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.0.0/24 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback0
C    192.168.3.0/24 is directly connected, Loopback0
R3#
```

批注 [stanley232]：通过配置路由过滤后，R3 将不能够学习到被拒绝的两条路由。

7、配置 R2 过滤 RIP 的路由：

```
R2(config)#access-list 2 deny 192.168.2.0 0.0.0.255
R2(config)#access-list 2 deny 192.168.3.0 0.0.0.255
R2(config)#access-list 2 permit any
R2(config)#router ospf 1
R2(config-router)#distribute-list 2 out rip
R2(config-router)#exit
```

批注 [stanley233]：配置路由过滤。

8、查看 R1 的路由表：

```
R1#show ip route
Gateway of last resort is not set
     172.16.0.0/30 is subnetted, 5 subnets
C       172.16.255.0 is directly connected, Serial1/1
C       172.16.0.0 is directly connected, Loopback0
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback0
C       172.16.3.0 is directly connected, Loopback0
O E2 192.168.255.0/24 [110/200] via 172.16.255.2, 00:19:20, Serial1/1
O E2 192.168.0.0/24 [110/200] via 172.16.255.2, 00:19:20, Serial1/1
O E2 192.168.1.0/24 [110/200] via 172.16.255.2, 00:19:20, Serial1/1
R1#
```

批注 [stanley234]：被过滤后的路由表内容。

9、实验完成。

CCNP Lab Manual

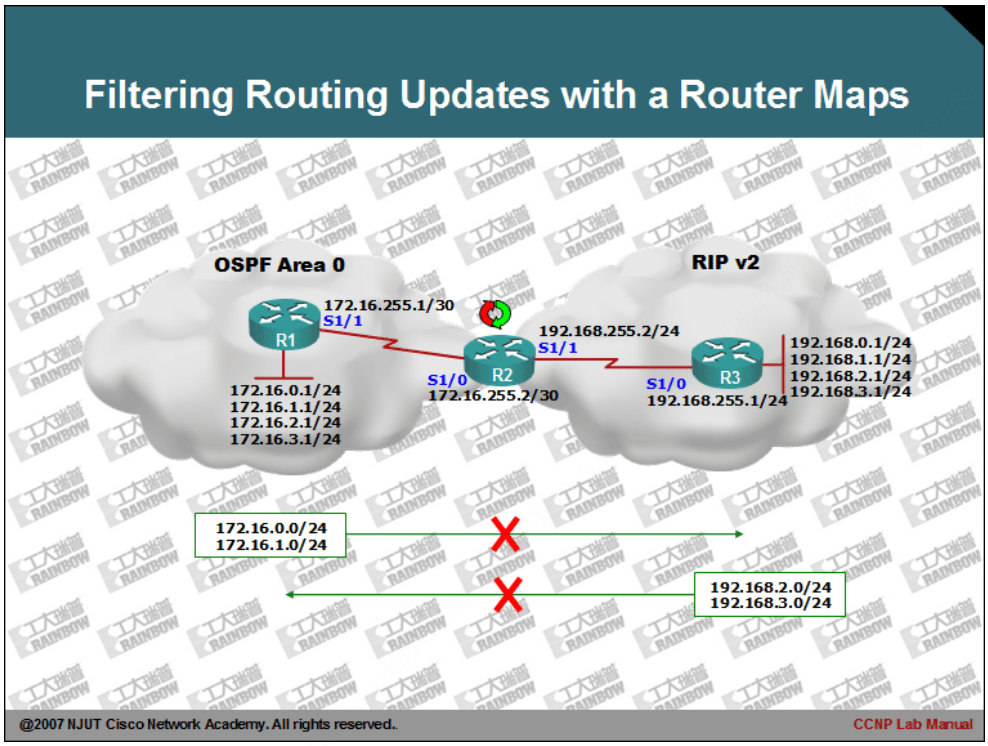
Lab 25. Filtering Routing Updates with a Router Maps

实验目的：

1、掌握基于 Route-map 的路由过滤配置方法。

2、掌握 route-map 的命令语法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、按照拓扑配置 OSPF 和 RIP v2 的路由协议。并关闭 RIP v2 的自动汇总。

3、在 R2 上配置路由重发布。

4、查看 R1 和 R3 的路由表：

```
R1#show ip route
Gateway of last resort is not set
     172.16.0.0/30 is subnetted, 5 subnets
C       172.16.255.0 is directly connected, Serial1/1
C       172.16.0.0 is directly connected, Loopback0
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback0
C       172.16.3.0 is directly connected, Loopback0
O E2 192.168.255.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.0.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.1.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.2.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
O E2 192.168.3.0/24 [110/200] via 172.16.255.2, 00:00:15, Serial1/1
```

```
R3#show ip route
Gateway of last resort is not set
     172.16.0.0/30 is subnetted, 5 subnets
R       172.16.255.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.0.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.1.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.2.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
R       172.16.3.0 [120/10] via 192.168.255.2, 00:00:01, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.0.0/24 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback0
C    192.168.3.0/24 is directly connected, Loopback0
```

5、根据拓扑的需要，在 R2 上配置路由过滤，以过滤 OSPF 的路由。配置如下：

```
R2(config)#access-list 1 deny 172.16.0.0 0.0.0.255
R2(config)#access-list 1 deny 172.16.1.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#
R2(config)#route-map ospf_to_rip permit 10
R2(config-route-map)#match ip address 1
```

批注 [stanley235]： 创建 route-map 并设定其名称为 ospf_to_rip。

其 permit 10 意思是指，如果下述 match 命令后面指定的条件成立的话，则其动作为允许。

类似于 ACL 的 permit。而且 route-map 跟 ACL 相同的是，在尾部也有隐藏的默认拒绝所有的条件。

批注 [stanley236]： 匹配 acl 1 所指定的网络。

```
R2(config-route-map)#exit
R2(config)#router rip
R2(config-router)#redistribute ospf 1 metric 10 route-map ospf_to_rip
R2(config-router)#exit
R2(config)#exit
```

批注 [stanley237]：在路由重布时，引用刚才配置 route-map 对重发布的路由进行过滤。

6、查看 R3 的路由，确认路由的学习：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 3 subnets
R       172.16.255.0 [120/10] via 192.168.255.2, 00:00:05, Serial1/0
R       172.16.2.0 [120/10] via 192.168.255.2, 00:00:05, Serial1/0
R       172.16.3.0 [120/10] via 192.168.255.2, 00:00:05, Serial1/0
C    192.168.255.0/24 is directly connected, Serial1/0
C    192.168.0.0/24 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback0
C    192.168.3.0/24 is directly connected, Loopback0
R3#
```

批注 [stanley238]：通过配置路由过滤后，R3 将不能够学习到被拒绝的两条路由。

7、配置 R2 过滤 RIP 的路由：

```
R2(config)#access-list 2 permit 192.168.2.0 0.0.0.255
R2(config)#access-list 2 permit 192.168.3.0 0.0.0.255
R2(config)#
R2(config)#route-map rip_to_ospf deny 10
R2(config-route-map)#match ip address 2
R2(config-route-map)#exit
R2(config)#route-map rip_to_ospf permit 20
R2(config-route-map)#exit
R2(config)#
R2(config)#router ospf 1
R2(config-router)#redistribute rip metric 200 subnets route-map rip_to_ospf
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley239]：本次使用 permit 方式进行匹配。

批注 [stanley240]：因为在 ACL 中使用是 permit 关键字。所以此处需要使用 dny 10 作为 route-map 的动作关键字。

批注 [stanley241]：指定需要 deny 的条件。

批注 [stanley242]：再次创建动作关键字为 permit 20 的 route-map，并且不追加任何条件语句。即匹配所有的条件。

批注 [stanley243]：在重发布时引用之前配置的 route-map

8、查看 R1 的路由表：

```
R1#show ip route
Gateway of last resort is not set
     172.16.0.0/30 is subnetted, 5 subnets
C       172.16.255.0 is directly connected, Serial1/1
C       172.16.0.0 is directly connected, Loopback0
C       172.16.1.0 is directly connected, Loopback0
```

```
C       172.16.2.0 is directly connected, Loopback0
C       172.16.3.0 is directly connected, Loopback0
O E2 192.168.255.0/24 [110/200] via 172.16.255.2, 00:19:20, Serial1/1
O E2 192.168.0.0/24 [110/200] via 172.16.255.2, 00:19:20, Serial1/1
O E2 192.168.1.0/24 [110/200] via 172.16.255.2, 00:19:20, Serial1/1
R1#
```

批注 [stanley244]: 被过滤后的路由表内容。

9、实验完成。

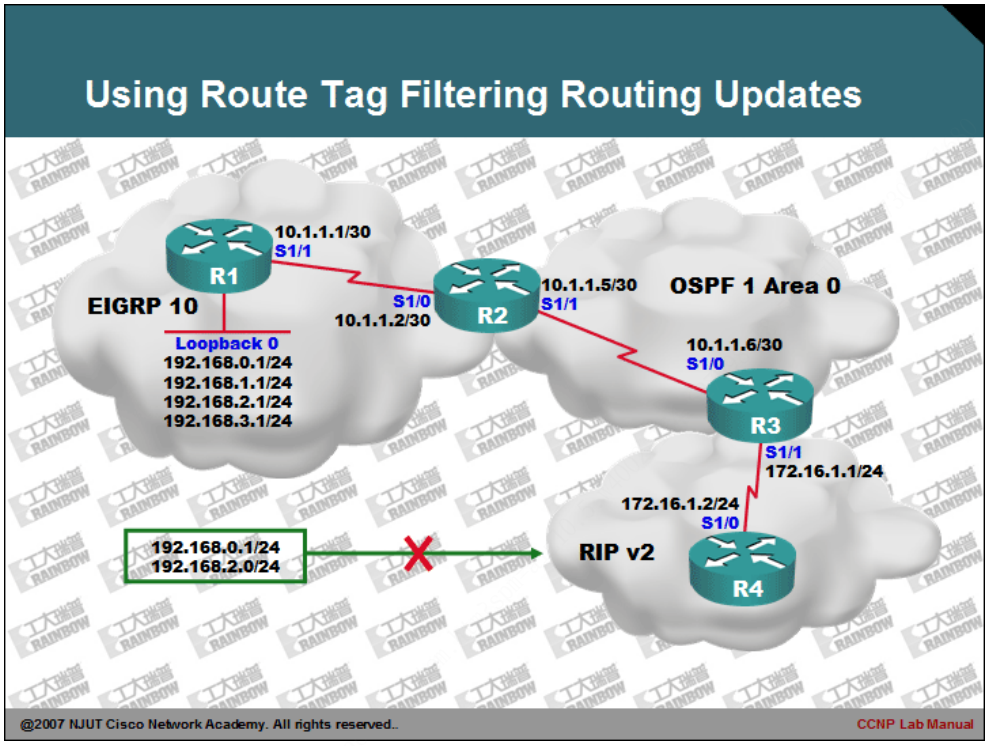
CCNP Lab Manual

Lab 26. Using Route Tag Filtering Routing Updates

实验目的：

1、掌握使用路由标记控制路由过滤。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 ping 命令确认连接。

2、配置 R2、R3 的路由双向重发布：

```
R2(config)#router ospf 1
R2(config-router)#redistribute eigrp 10 subnets
R2(config-router)#exit
R2(config)#
R2(config)#router eigrp 10
R2(config-router)#redistribute ospf 1 metric 100000 100 255 1 1500
R2(config-router)#exit
R2(config)#exit
```

```
R3(config)#router ospf 1
R3(config-router)#redistribute rip subnets
R3(config-router)#exit
R3(config)#
R3(config)#router rip
R3(config-router)#redistribute ospf 1 metric 10
R3(config-router)#exit
R3(config)#
```

3、在 R4 上查看路由表，确认路由重发布：

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial1/0
     10.0.0.0/30 is subnetted, 2 subnets
R       10.1.1.0 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R       10.1.1.4 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R    192.168.0.0/24 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R    192.168.1.0/24 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R    192.168.2.0/24 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R    192.168.3.0/24 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R4#
```

批注 [stanley245]: 通过重发布学到的非 RIP 区域路由。

4、根据拓扑配置得知，192.168.0.0/24 和 192.168.2.0/24 的网络不允许被 R4 学习。除了 Distribute-list 或 Route-map 配置可以了实现此路由过滤功能。也可以通过配置路由标记，来实现路由过滤的功能。

5、使用路由标记的过滤，分为两个步骤。一、服务器端路由器配置标记。二、

客户端路由器根据标记进行过滤。

6、在 R2 上配置分配路由标记：

```
R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R2(config)#
R2(config)#route-map set_tag permit 10
R2(config-route-map)#match ip address 1
R2(config-route-map)#set tag 1
R2(config-route-map)#exit
R2(config)#
R2(config)#route-map set_tag permit 20
R2(config-route-map)#exit
R2(config)#
R2(config)#router ospf 1
R2(config-router)#redistribute eigrp 10 subnets route-map set_tag
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley246]：使用 ACL 标识出需要设置标记的路由。

批注 [stanley247]：为匹配 ACL 1 的路由条目，分配标记为 1。

批注 [stanley248]：在路由重发布时调用路由图，进行标记的嵌入。

7、在 R3 上，配置 route-map 通过标记来进行路由过滤：

```
R3(config)#route-map match_tag deny 10
R3(config-route-map)#match tag 1
R3(config-route-map)#exit
R3(config)#
R3(config)#route-map match_tag permit 20
R3(config-route-map)#exit
R3(config)#
R3(config)#router rip
R3(config-router)#redistribute ospf 1 metric 10 route-map match_tag
R3(config-router)#exit
R3(config)#exit
R3#
```

批注 [stanley249]：对于标记为 1 的路由，进行过过滤外理。

批注 [stanley250]：其它的路由无条件转发。

批注 [stanley251]：在路由重发布时调用路由图进行了过滤。

8、查看 R4 的路由表，确认路由过滤：

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial1/0
     10.0.0.0/30 is subnetted, 2 subnets
R       10.1.1.0 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R       10.1.1.4 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
```

```
R    192.168.1.0/24 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R    192.168.3.0/24 [120/10] via 172.16.1.1, 00:00:00, Serial1/0
R4#
```

批注 [stanley252]: R4 的路由表显示路由过滤成功。

9、路由标记可以简单的实现路由预先分类，客户端仅需要简单匹配标记而不需要编写大量的 ACL 来标识路由。通过此配置，可以有效的维护网络的路由更新。

10、实验完成。

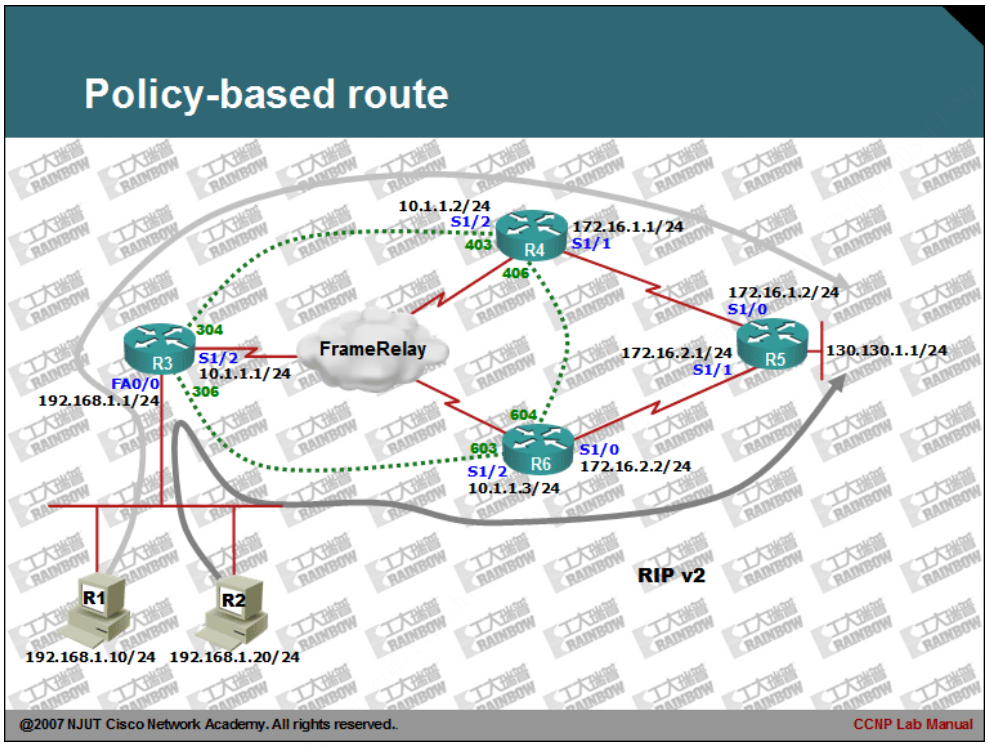
Lab 27. Policy-based route

实验目的：

1、掌握策略路由配置。

2、理解根据源址来路由转发的配置。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、其中 R1 和 R2 模拟成主机。配置如下：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.10 255.255.255.0
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#ip address 192.168.1.20 255.255.255.0
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

3、其中帧中继网络采用默认配置，具体如下：

```
R3(config)#interface serial 1/2
R3(config-if)#ip address 10.1.1.1 255.255.255.0
R3(config-if)#encapsulation frame-relay
R3(config-if)#exit
```

```
R4(config)#interface s1/2
R4(config-if)#ip address 10.1.1.2 255.255.255.0
R4(config-if)#encapsulation frame-relay
R4(config-if)#exit
```

```
R6(config)#interface s1/2
R6(config-if)#encapsulation frame-relay
R6(config-if)#ip address 10.1.1.3 255.255.255.0
```

4、在 R3、R4、R5、R6 启用 RIP v2 协议，同时关闭自动总结。

5、查看 R3 的路由表：

```
R3#show ip route

     172.16.0.0/24 is subnetted, 2 subnets
R       172.16.1.0 [120/1] via 10.1.1.2, 00:00:01, Serial1/2
R       172.16.2.0 [120/1] via 10.1.1.3, 00:00:14, Serial1/2
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/2
     130.130.0.0/24 is subnetted, 1 subnets
R       130.130.1.0 [120/2] via 10.1.1.2, 00:00:01, Serial1/2
                    [120/2] via 10.1.1.3, 00:00:14, Serial1/2
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

批注 [stanley253]：此处显示到达 R3 的 130.130.1.0/24 的网络有多条路由。并且采用均衡负载进行转发数据包。

```
R3#
```

6、在 R3 的路由器使用如下命令，关闭快速转发。

```
R3(config)#no ip cef
```

批注 [stanley254]：关闭 Cisco Express Forwarding。便于观察路由路径。

7、在 R1 上跟踪到达 130.130.1.0/24 网络的数据包：

```
R1#traceroute 130.130.1.1

Type escape sequence to abort.
Tracing the route to 130.130.1.1

  1 192.168.1.1 52 msec 96 msec 48 msec
  2 10.1.1.2 216 msec
    10.1.1.3 240 msec
    10.1.1.2 120 msec
  3 172.16.2.1 264 msec
    172.16.1.2 216 msec *
R1#
```

批注 [stanley255]：跟踪到达 130.130.1.1 的数据包，观察路径。

批注 [stanley256]：此处同时出现 10.1.1.2 和 10.1.1.3，表示 R1 正在通过 R3 使用两条路径转发数据包。

8、在 R2 上跟踪到达 130.130.1.0/24 网络的数据包：

```
R2#traceroute 130.130.1.1

Type escape sequence to abort.
Tracing the route to 130.130.1.1

  1  *
    192.168.1.1 96 msec 72 msec
  2 10.1.1.2 192 msec
    10.1.1.3 120 msec
    10.1.1.2 144 msec
  3 172.16.2.1 264 msec
    172.16.1.2 216 msec *
```

批注 [stanley257]：R2 的数据包也与 R1 一样被 R3 使用相同的方式进行数据转发。

9、根据拓扑进行策略路由的配置。在 R3 上策略路由配置如下所示：

```
R3(config)#access-list 10 permit host 192.168.1.10
R3(config)#access-list 20 permit host 192.168.1.20
R3(config)#
R3(config)#route-map pbd permit 10
R3(config-route-map)#
R3(config-route-map)#match ip address 10
R3(config-route-map)#set ip next-hop 10.1.1.2
R3(config-route-map)#
R3(config-route-map)#exit
R3(config)#
R3(config)#route-map pbd permit 20
```

批注 [stanley258]：通过 ACL 标识出 R1 的数据包。

批注 [stanley259]：R2 的数据包。

批注 [stanley260]：配置名为 PBD 的 route-map。

批注 [stanley261]：如果源地址匹配 ACL 10，则指定下一跳为 10.1.1.2。

```
R3(config-route-map)#
R3(config-route-map)#match ip address 20
R3(config-route-map)#set ip next-hop 10.1.1.3
R3(config-route-map)#
R3(config-route-map)#exit
R3(config)#route-map pbd permit 30
R3(config-route-map)#exit
R3(config)#
```

批注 [stanley262]：如果源地址匹配 ACL 20，则指定下一跳为 10.1.1.3。

批注 [stanley263]：对于其它的数据包采用默认转发方式进行转发。

10、配置策略到接口：

```
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip policy route-map pbd
R3(config-if)#
```

批注 [stanley264]：将策略指定接口上。

11、再次在 R1 和 R3 上跟踪数据包路径：

```
R1#traceroute 130.130.1.1
Type escape sequence to abort.
Tracing the route to 130.130.1.1
  1 192.168.1.1 132 msec 72 msec 72 msec
  2 10.1.1.2 168 msec 144 msec 144 msec
  3 172.16.1.2 168 msec *  312 msec
R1#
```

批注 [stanley265]：此时 R1 的数据包第二跳的路径已经变为从 R4 的 10.1.1.2，而且不再出现 10.1.1.3 的地址。

```
R2#traceroute 130.130.1.1
Type escape sequence to abort.
Tracing the route to 130.130.1.1
  1 192.168.1.1 48 msec 68 msec 72 msec
  2 10.1.1.3 144 msec 192 msec 144 msec
  3 172.16.2.1 216 msec *  216 msec
R2#
```

12、通过配置策略路由，可以根据源地址进行数据包的路由。

13、实验完成。

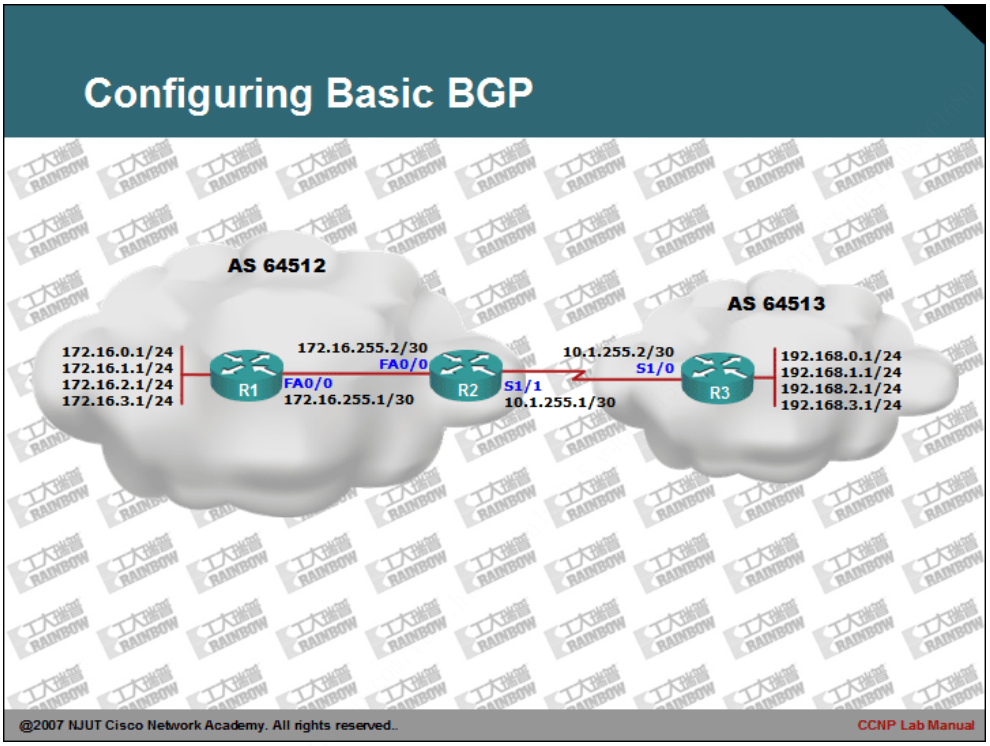
Lab 28. Configuring Basic BGP

实验目的：

1、掌握 BGP 的基本配置方法。

2、掌握如何查看 BGP 的各种配置信息。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、在 R1、R2 和 R3 配置 BGP 路由协议,具体配置如下：

```
R1(config)#router bgp 64512
R1(config-router)#neighbor 172.16.255.2 remote-as 64512
R1(config-router)#
R1(config-router)#network 172.16.255.0 mask 255.255.255.252
R1(config-router)#network 172.16.0.0 mask 255.255.255.0
R1(config-router)#network 172.16.1.0 mask 255.255.255.0
R1(config-router)#network 172.16.2.0 mask 255.255.255.0
R1(config-router)#network 172.16.3.0 mask 255.255.255.0
R1(config-router)#exit
R1(config)#
```

批注 [stanley266]：启用 AS 64512 自动系统的 BGP 路由

批注 [stanley267]：确定邻居以及邻居的 AS 号。

配置邻居的 AS 号的目的，是为了与本地路由器所在 AS 号进行比较，确定需要创建是 iBGP 还是 eBGPR 的邻居邻居。

```
R2(config)#router bgp 64512
R2(config-router)#neighbor 172.16.255.1 remote-as 64512
R2(config-router)#neighbor 10.1.255.2 remote-as 64513
R2(config-router)#
R2(config-router)#network 172.16.255.0 mask 255.255.255.252
R2(config-router)#network 10.1.255.0 mask 255.255.255.252
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley268]：向 BGP 中注入带有具体长度的直网络路由。

批注 [stanley269]：由于指定的 10.1.255.2 路由器的 AS 号与地址不同。
所以此邻居将被识别为 eBGP 的邻居对等体关系。

```
R3(config)#router bgp 64513
R3(config-router)#neighbor 10.1.255.1 remote-as 64512
R3(config-router)#
R3(config-router)#network 10.1.255.0 mask 255.255.255.252
R3(config-router)#network 192.168.0.0
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#exit
R3(config)#
```

批注 [stanley270]：向 BGP 中注入直连路由，不带子网掩码的配置方法。

批注 [stanley271]：指出当前的 BGP 的对等体的 route id，以及对等体所处的 AS 编号，及邻居关系为 iBGP 关系。

3、查看 BGP 的邻居关系：

```
R1#show ip bgp neighbors
BGP neighbor is 172.16.255.2,  remote AS 64512, internal link
  BGP version 4, remote router ID 172.16.255.2
  BGP state = Established, up for 00:29:25
  Last read 00:00:24, hold time is 180, keepalive interval is 60 seconds
```

批注 [stanley272]：邻居关系的状态。

批注 [stanley273]：HoldTime 和 Keepalive 计时器。其主要的作用是维持邻居关系。

```
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          4
    Keepalives:            32         32
    Route Refresh:          0          0
    Total:                 34         37
  Default minimum time between advertisement runs is 5 seconds
.....
```

批注 [stanley274]：BGP 的几种数据包的发送接收数量。

4、查看简洁 BGP 汇总信息：

```
R2#show ip bgp summary
BGP router identifier 172.16.255.2, local AS number 64512
BGP table version is 19, main routing table version 19
10 network entries using 1010 bytes of memory
11 path entries using 528 bytes of memory
3 BGP path attribute entries using 180 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1742 total bytes of memory
BGP activity 14/4 prefixes, 16/5 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.255.2      4 64513      47      49       19    0    0 00:10:15        5
172.16.255.1    4 64512      42      45       19    0    0 00:37:53        4
R2#
```

批注 [stanley275]：BGP 的对等体列表。
目前 state 列显示数字，表示从此对等体学习到路由的数量。

其中 State 一列。还会出现：IDLE，ACTIVE 状态。
IDLE 状态表示，对等体关系尚未建立。

ACTIVE 状态邻居关系表示 BGP 协议正在处于邻居创建过程中，但此时邻居关系尚未完成创建。

5、查看 R1 的路由表：

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.255.0/30 is directly connected, FastEthernet0/0
C       172.16.0.0/24 is directly connected, Loopback0
C       172.16.1.0/24 is directly connected, Loopback0
C       172.16.2.0/24 is directly connected, Loopback0
```

```
C       172.16.3.0/24 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 1 subnets
B       10.1.255.0 [200/0] via 172.16.255.2, 00:48:22
B    192.168.0.0/24 [200/0] via 10.1.255.2, 00:22:27
B    192.168.1.0/24 [200/0] via 10.1.255.2, 00:22:27
B    192.168.2.0/24 [200/0] via 10.1.255.2, 00:22:27
B    192.168.3.0/24 [200/0] via 10.1.255.2, 00:22:27
R1#
```

批注 [stanley276]: BGP 学习的路由。

6、另外一些命令：

```
R1#clear ip bgp *

R1#clear ip bgp 172.16.255.2

R1#clear ip bgp * soft
```

批注 [s277]: 清除BGP的路由表，邻居关系重置。

批注 [stanley278]: 仅针对 172.16.255.2 对等体的 BGP 会话进行重置。

批注 [stanley279]: 软清除命令。本条命令可以直接刷路由表，而不重置 BGP 的邻居关系，即不会重置 TCP 的连接关系。

7、实验完成。

CCNP Lab Manual

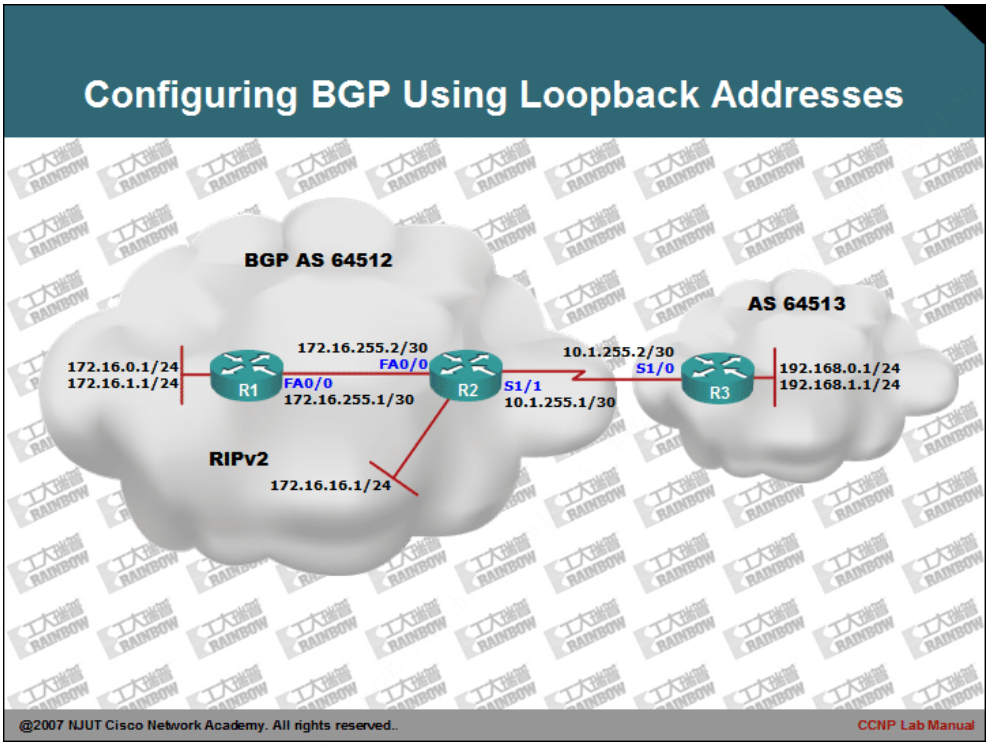
Lab 29. Configuring BGP Using Loopback Addresses

实验目的：

1、掌握基于回环口的 BGP 的邻居关系建立的配置方法。

2、理解需要使用回环口为目的。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置 AS 64512 自治系统的 RIPv2 路由协议。

```
R1(config)#router rip
R1(config-router)#network 172.16.0.0
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#exit
```

```
R2(config)#router rip
R2(config-router)#no auto-summary
R2(config-router)#version 2
R2(config-router)#network 172.16.0.0
R2(config-router)#exit
```

3、首先在 R1 和 R2 上使用回环口创建邻居关系，配置如下：

```
R1(config)#router bgp 64512
R1(config-router)#network 172.16.0.0 mask 255.255.255.0
R1(config-router)#network 172.16.1.0 mask 255.255.255.0
R1(config-router)#neighbor 172.16.16.1 remote-as 64512
R1(config-router)#exit
```

批注 [stanley280]: 创建 BGP 对等体，使用 R2 回环口的地址。

```
R2(config)#router bgp 64512
R2(config-router)#network 172.16.255.0 mask 255.255.255.252
R2(config-router)#network 10.1.255.0 mask 255.255.255.252
R2(config-router)#
R2(config-router)#neighbor 172.16.0.1 remote-as 64512
R2(config-router)#exit
```

批注 [stanley281]: 使用 R1 的回环口地址创建邻居关系。

4、由于 BGP 在创建对等体时，需要时间较长。所以，需要等待一段时间。然后再查看 R1 和 R2 的 BGP Summary 信息。

```
R1#show ip bgp summary

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.16.1     4 64512       0       0        0    0    0 never    Active
R1#
```

批注 [stanley282]: Active 状态指出此时 BGP 正在尝试创建邻居关系。

```
R2#show ip bgp summary

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.0.1      4 64512       0       0        0    0    0 never    Active
```

```
R2#
```

5、在 R1 路由器开启对 BGP 的调试：

```
R1#debug ip bgp in
*Mar 30 11:42:34.607: BGP: 172.16.16.1 multihop open delayed 19731ms (no route)
*Mar 30 11:42:54.339: BGP: 172.16.16.1 multihop open delayed 17735ms (no route)
*Mar 30 11:43:12.075: BGP: 172.16.16.1 multihop open delayed 17459ms (no route)
*Mar 30 11:43:29.535: BGP: 172.16.16.1 multihop open delayed 14687ms (no route)
```

批注 [stanley283]：对接收到的 BGP 的数据包进行分析。

6、由于 R1 和 R2 是同一个自治系统，所以我们使用 RIPv2 协议来解决路由不可达的问题，同时还要在 BGP 协议中指出使用回环口配置邻居关系，具体配置如下：

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#
R1(config-router)#network 172.16.0.0
R1(config-router)#exit
R1(config)#
R1(config)#router bgp 64512
R1(config-router)#neighbor 172.16.16.1 update-source loopback 0
R1(config-router)#exit
```

批注 [stanley284]：可以看出，此时，BGP 已经发现使用对方回环口创建邻居关系。BGP 将其称为**多跳**。而邻居创建不成功的主要原因是：**no route**，即没有路由可以到达邻居的回环口。无法进行 TCP 的三次握手。

批注 [stanley285]：由于 AS 64512 自治内存在无类路由，所以此处必须启用 Version 2 版本。

批注 [stanley286]：指定使用本地回环口创建邻居关系。

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 172.16.0.0
R2(config-router)#exit
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 172.16.0.1 update-source loopback 0
R2(config-router)#exit
```

7、稍等片刻或是直接 clear ip bgp *后，再次查看 R1 的 BGP summary 信息：

```
R1#sh ip bgp summary
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.16.1     4 64512       5       5        6    0    0 00:00:20        2
R1#
```

批注 [stanley287]：此时，已经成功的创建对等体关系。

8、再次配置 R2 与 R3 使用回环口创建 eBGP 邻居关系：

```
R2(config)#router bgp 64512
R2(config-router)#neighbor 192.168.0.1 remote-as 64513
R2(config-router)#neighbor 192.168.0.1 update-source loopback 0
R2(config-router)#neighbor 192.168.0.1 ebgp-multihop 2
R2(config-router)#exit
R2(config)#ip route 192.168.0.1 255.255.255.255 10.1.255.2
```

批注 [stanley288]：指出 eBGP 的邻居地址存在多跳特性。

批注 [stanley289]：由于 R2 与 R3 处于不同的自治系统中，所以建立配置静态路由。

```
R3(config)#router bgp 64513
R3(config-router)#neighbor 172.16.16.1 remote-as 64512
R3(config-router)#neighbor 172.16.16.1 update-source loopback 0
R3(config-router)#neighbor 172.16.16.1 ebgp-multihop 2
R3(config-router)#
R3(config-router)#network 192.168.0.0
R3(config-router)#network 192.168.1.0
R3(config-router)#network 10.1.255.0 mask 255.255.255.252
R3(config-router)#exit
R3(config)#ip route 172.16.16.1 255.255.255.255 10.1.255.1
```

9、在 R2 上观察 BGP 的邻居关系状态：

```
R2#show ip bgp summary
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.0.1      4 64512      19      20        9    0    0 00:14:11        2
192.168.0.1     4 64513       5       6        9    0    0 00:00:10        3
R2#
```

批注 [stanley290]: BGP 的邻居关系已经被成功创建成功。

10、实验完成。

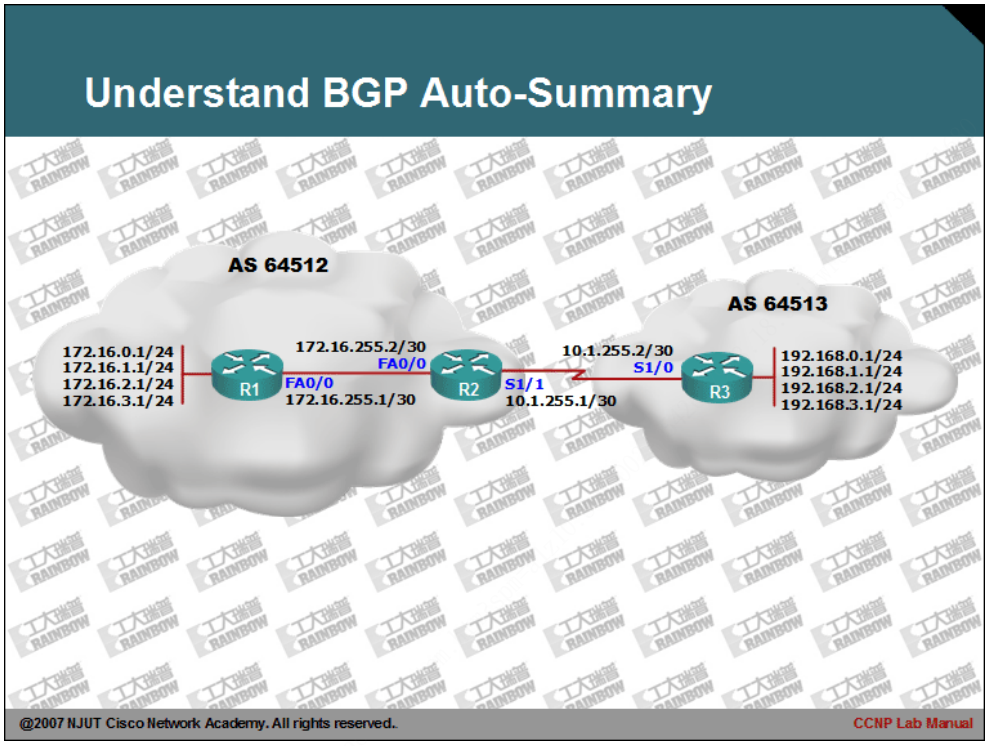
CCNP Lab Manual

Lab 30. Understand BGP Auto-Summary

实验目的：

1、理解 BGP 的自动汇总特性。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、首先配置各路由器的邻居关系，并通过相关命令确认邻居关系的状态。配置如下：

```
R1(config)#router bgp 64512
R1(config-router)#neighbor 172.16.255.2 remote-as 64512
R1(config-router)#exit
```

```
R2(config)#router bgp 64512
R2(config-router)#neighbor 172.16.255.1 remote-as 64512
R2(config-router)#neighbor 10.1.255.2 remote-as 64513
R2(config-router)#exit
```

```
R3(config)#router bgp 64513
R3(config-router)#neighbor 10.1.255.1 remote-as 64512
R3(config-router)#exit
```

9、在 R2 上观察 BGP 的邻居关系状态：

```
R2#sh ip bgp summary
BGP router identifier 172.16.16.1, local AS number 64512
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.255.2      4 64513       5       5        1    0    0 00:01:01        0
172.16.255.1    4 64512       5       5        1    0    0 00:01:46        0
R2#
```

4、查看 R1 的 BGP 的协议属性：

```
R1#show ip protocols
Routing Protocol is "bgp 64512"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    172.16.255.2
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: external 20 internal 200 local 200
```

批注 [stanley291]：同步规则默认是禁用的。

注意：在低于 12.3 以下 IOS 的版下，同步规则默认是启用的。

批注 [stanley292]：自动汇总属性默认是禁用的。

注意：在低于 12.2 以下的 IOS 的版上，自动汇总是默认启用的。

```
R1#
```

5、在 R1 作如下配置：

```
R1(config)#router bgp 64512
R1(config-router)#network 172.16.0.0
R1(config-router)#exit
```

批注 [stanley293]：宣告 172.16.0.0 的主类网络路由。

6、在 R2 上使用 clear ip bgp * soft 命令，加快 BGP 的收敛后，查看 R2 的路由表和 summary 信息：

```
R2#show ip bgp summary

BGP router identifier 172.16.16.1, local AS number 64512
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.255.2      4 64513      12      12        1    0    0 00:08:29        0
172.16.255.1    4 64512      13      13        1    0    0 00:09:14        0
R2#
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.255.0/30 is directly connected, FastEthernet0/0
C       172.16.16.0/24 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/1
R2#
```

批注 [stanley294]：此条信息显示，R2 并没有从 R1 学习到任何路由条目。

7、问题分析：BGP 协议在将某路由通告给自己的邻居对等体时，会检查路由是否同步和本地路由表中是否已经存在此条路由。本实验中 R2 没有学习到 R1 的路由的主要问题并不是同步，而是 R1 的路由表中没有关于 172.16.0.0/16 子网的路由。

8、在 R1 上查看 BGP 对 172.16.0.0/16 网络路由描述：

```
R1#show ip bgp 172.16.0.0

% Network not in table

R1#
```

批注 [stanley295]：BGP 指出 172.16.0.0/16 不在路由表中。

9、在 R1 作如下配置：

```
R1(config)#router bgp 64512
```

```
R1(config-router)#auto-summary
R1(config-router)#exit
R1(config)#exit
```

批注 [stanley296]：开启自动总结功能。

10、再次查看 R2 路由表：

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
C       172.16.255.0/30 is directly connected, FastEthernet0/0
C       172.16.16.0/24 is directly connected, Loopback0
B       172.16.0.0/16 [200/0] via 172.16.255.1, 00:01:23
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/1
R2#
R2#show ip bgp summary

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.255.2      4 64513      19      20        2    0    0 00:15:27        0
172.16.255.1    4 64512      21      20        2    0    0 00:16:11        1
R2#
```

批注 [stanley297]：此时 R2 路由器学习到 1 条汇总路由。

11、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

B    172.16.0.0/16 [20/0] via 10.1.255.1, 00:02:26
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
C    192.168.0.0/24 is directly connected, Loopback0
C    192.168.1.0/24 is directly connected, Loopback0
R3#
```

12、实验总结：BGP 的自动总结特性，并不是像普通距离矢量协议一样，在主类的边界进行汇总。

BGP 的自动汇总，其主要是将本地多个相同主类网络下的无类路由向主类网络进行汇总，并且向邻居路由器通告此条路由。而不管其本身是否处于主类边界。

13、实验完成。

CCNP Lab Manual

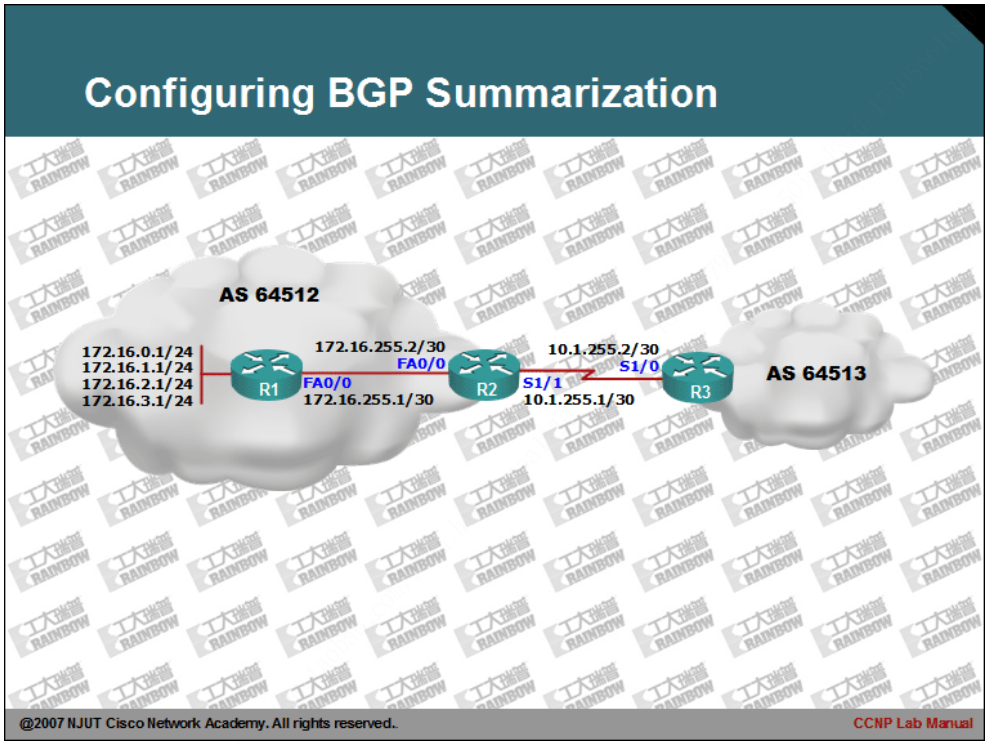
Lab 31. Configuring BGP Summarization

实验目的：

1、掌握使用指向 NULL0 接口的静态路由的汇总配置方法。

2、掌握使用聚合属性的路由汇总配置方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通性。

2、配置各台路由器的 BGP 协议，并且正确宣告相应的网络：

3、查看 R3 路由器的路由表信息：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:03:15
B       172.16.0.0/24 [20/0] via 10.1.255.1, 00:02:45
B       172.16.1.0/24 [20/0] via 10.1.255.1, 00:02:45
B       172.16.2.0/24 [20/0] via 10.1.255.1, 00:02:45
B       172.16.3.0/24 [20/0] via 10.1.255.1, 00:02:45
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

4、以通过路由汇总配置，有效的减少路由表的大小，提高路由效率。因此在 R1 路由器作如下的配置：

```
R1(config)#ip route 172.16.0.0 255.255.252.0 null 0
R1(config)#
R1(config)#router bgp 64512
R1(config-router)#network 172.16.0.0 mask 255.255.252.0
R1(config-router)#exit
```

批注 [stanley298]： 配置一个条指向 NULL0 接口的路由。注意此条路由为汇总的网络号。

批注 [stanley299]： 使用 network 命令将指向 NULL 0 接口的路由，宣告给 BGP 对等体。

5、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 6 subnets, 3 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:07:18
B       172.16.0.0/24 [20/0] via 10.1.255.1, 00:06:48
B       172.16.0.0/22 [20/0] via 10.1.255.1, 00:00:01
B       172.16.1.0/24 [20/0] via 10.1.255.1, 00:06:48
B       172.16.2.0/24 [20/0] via 10.1.255.1, 00:06:48
B       172.16.3.0/24 [20/0] via 10.1.255.1, 00:06:48
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
```

批注 [stanley300]： 此时 R3 路由已经可以学习到被汇总的路由。

```
R3#
```

6、BGP 的 network 命令与 OSPF 或是其它的 IGP 不同的是：**BGP 当检测到本地有 network 命令，首先 BGP 会检查本地路由表，查看是否此条路由存在，如果有，则将此条路由通告给对等体，否则忽略此条 network 命令。**

7、另外需要注意的是，虽然在 R3 学习了/22 位子网汇总路由，但是其它的/24 位网络具体路由也同时出现的路由表，因此还需要在 R1 上作如下配置：

```
R1(config)#router bgp 64512
R1(config-router)#no network 172.16.0.0 mask 255.255.255.0
R1(config-router)#no network 172.16.1.0 mask 255.255.255.0
R1(config-router)#no network 172.16.2.0 mask 255.255.255.0
R1(config-router)#no network 172.16.3.0 mask 255.255.255.0
R1(config-router)#exit
R1(config)#
```

8、查看 R3 的路由表：

```
R3#show ip route
Gateway of last resort is not set
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:23:36
B       172.16.0.0/22 [20/0] via 10.1.255.1, 00:16:20
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

9、测试汇总路由有效性：

```
R3#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/184/216 ms
R3#
```

10、虽然通过指向 NULL 0 口的路由进行配置 BGP 的汇总非常的简单，而且易于理解，但是不利于排错，因为其它 BGP 的路由器无法获知路由在何处汇总的。因此，建议使用 BGP 的聚合方法进行配置汇总。

11、在 R1 上将的指向 NULL 0 的接口静态路由和 BGP 的下的针对指向 NULL 0 口的静态路由的宣告给 no 掉。同时，在 R1 上将四个回环口的子网重新 network 宣告。

12、在 R1 路由器实施聚合的配置：

```
R1(config)#router bgp 64512
R1(config-router)#aggregate-address 172.16.0.0 255.255.252.0 summary-only
R1(config-router)#
```

批注 [stanley301]：对 172.16.0.0 的四个 24 位子网路由汇总成一条 172.16.0.0/22 位的汇总路由。

summary-only 的主要目的是，仅发送汇总路由，而不发送具体路由。

13、查看 R3 的路由表：

```
R3#show ip route
Gateway of last resort is not set
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:18:08
B       172.16.0.0/22 [20/0] via 10.1.255.1, 00:02:00
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

批注 [stanley302]：路由已经被汇总。

14、查看汇总路由的属性：

```
R3#show ip bgp 172.16.0.0
BGP routing table entry for 172.16.0.0/22, version 32
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  64512, (aggregated by 64512 172.16.0.1)
    10.1.255.1 from 10.1.255.1 (172.16.255.1)
      Origin IGP, localpref 100, valid, external, atomic-aggregate, best
R3#
```

批注 [stanley303]：显示了谁聚合了此条路由。
此处显示是由：64512 自治系统的 172.16.0.1 聚合了此条路由。172.16.0.1 为路由 ID。

15、测试汇总路由的有效性：

```
R3#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/128/168 ms
R3#
```

16、实验完成。

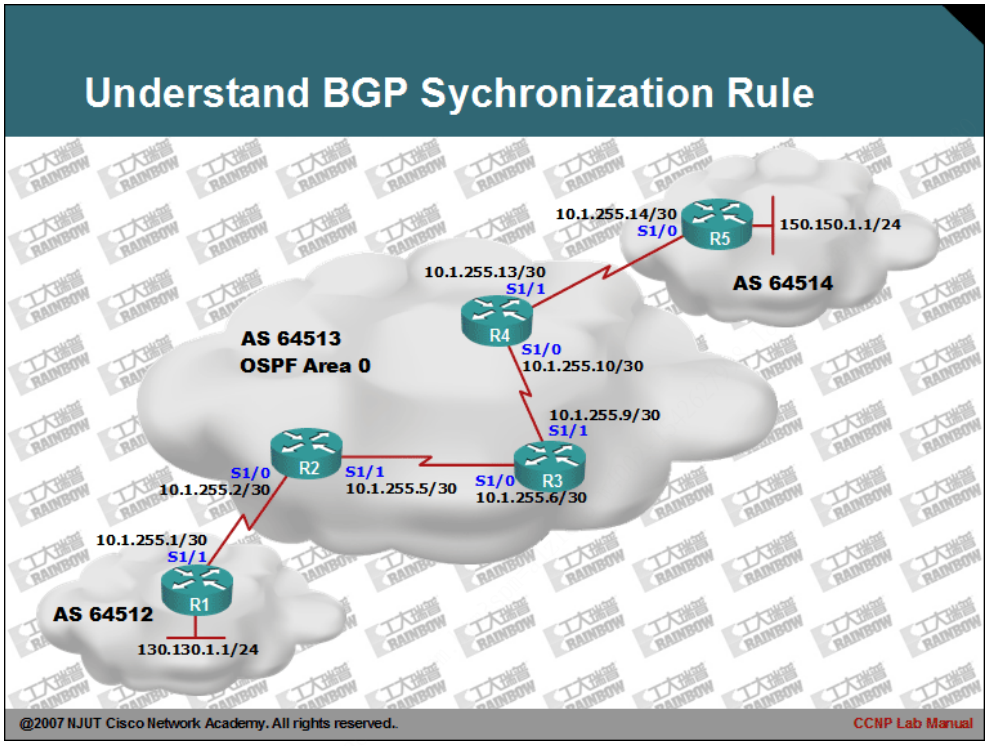
CCNP Lab Manual

Lab 32. Understand BGP Sychronization Rule

实验目的：

1、深入理解 BGP 的同步规则。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置各路由器的 BGP 协议：

```
R3#show ip protocols
Routing Protocol is "bgp 64513"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    10.1.255.5
    10.1.255.10
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.255.5           200      00:02:52
    10.1.255.10          200      00:29:53
  Distance: external 20 internal 200 local 200

R3#
```

批注 [stanley304]:

此时同步规则被关闭。

4、查看 R2 与 R4 的路由表：

```
R2#show ip route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 3 subnets
C       10.1.255.4 is directly connected, Serial1/1
C       10.1.255.0 is directly connected, Serial1/0
B       10.1.255.8 [200/0] via 10.1.255.6, 00:06:24
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 10.1.255.1, 00:07:20
R2#
```

批注 [stanley305]: 在 R2 的路由表中，并没有发现 150.150.1.0/24 和 130.130.1.12/30 的网络路由。

```
R4#show ip route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 3 subnets
B       10.1.255.4 [200/0] via 10.1.255.9, 00:06:20
```

```
C       10.1.255.12 is directly connected, Serial1/1
C       10.1.255.8 is directly connected, Serial1/0
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 10.1.255.14, 00:06:20
R4#
```

批注 [stanley306]：在 R4 的路由表，并没有也同样无法发现 130.130.1.0/24 和 10.1.255.4/30 的网络路由。

5、出现这种问题的主要原因是：**BGP 规则：从 iBGP 对等体学习到路由，永远不会向其它的 iBGP 对等体通告**。正是因为这个原因，所以 R2 和 R4 无法学习完整的网络路由。

6、在 R2 和 R4 的路由器上配置 iBGP 的邻居关系，配置如下：

```
R2(config)#router bgp 64513
R2(config-router)#neighbor 10.1.255.10 remote-as 64513
R2(config-router)#exit
R2(config)#exit
```

批注 [stanley307]：配置与 R4 的 iBGP 邻居关系。

```
R4(config)#router bgp 64513
R4(config-router)#neighbor 10.1.255.5 remote-as 64513
R4(config-router)#exit
R4(config)#exit
```

7、再次查看 R2 和 R4 的路由表：

```
R2#show ip route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 4 subnets
C       10.1.255.4 is directly connected, Serial1/1
C       10.1.255.0 is directly connected, Serial1/0
B       10.1.255.12 [200/0] via 10.1.255.10, 00:05:51
B       10.1.255.8 [200/0] via 10.1.255.6, 00:06:03
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 10.1.255.1, 00:06:03
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [200/0] via 10.1.255.14, 00:05:39
R2#
```

批注 [stanley308]：R2 路由器已经成功学习到整个网络的路由。

```
R4#show ip route

     10.0.0.0/30 is subnetted, 4 subnets
B       10.1.255.4 [200/0] via 10.1.255.5, 00:00:06
B       10.1.255.0 [200/0] via 10.1.255.5, 00:00:06
C       10.1.255.12 is directly connected, Serial1/1
C       10.1.255.8 is directly connected, Serial1/0
```

批注 [stanley309]：**注意下一跳，并不是最佳路由。**

可以使用 ping 命令，会发现无法 ping 通 10.1.255.4/30 的网络。

```
      150.150.0.0/24 is subnetted, 1 subnets
B        150.150.1.0 [20/0] via 10.1.255.14, 00:16:40
R4#
```

批注 [stanley310]：R4 路由器仍然无法学习完整路由。

8、查看 bgp 的内部路由表：

```
R4#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
* i10.1.255.0/30    10.1.255.5               0    100      0 i
* i10.1.255.4/30    10.1.255.5               0    100      0 i
*>i                 10.1.255.9               0    100      0 i
* i10.1.255.8/30    10.1.255.9               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*  10.1.255.12/30   10.1.255.14              0             0 64514 i
*>                  0.0.0.0                  0         32768 i
* i130.130.1.0/24   10.1.255.1               0    100      0 64512 i
*> 150.150.1.0/24   10.1.255.14              0             0 64514 i
R4#
```

批注 [stanley311]：R4 学习到 130.130.1.0/24 网络路由。但 BGP 认为其不是最佳路由。

9、查看 130.130.1.0/24 网络路由，具体信息：

```
R4#show ip bgp 130.130.1.0
BGP routing table entry for 130.130.1.0/24, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  64512
    10.1.255.1 (inaccessible) from 10.1.255.5 (10.1.255.5)
      Origin IGP, metric 0, localpref 100, valid, internal
```

批注 [stanley312]：下一跳不可达。

10、继续分析：

```
R4#show ip bgp 10.1.255.0
.............
  Advertised to non peer-group peers:
  10.1.255.14
  Local
    10.1.255.5 from 10.1.255.5 (10.1.255.5)
      Origin IGP, metric 0, localpref 100, valid, internal, best
R4#ping 10.1.255.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

批注 [stanley313]：虽然是最佳路由。但是注意其下一跳是错误的。

批注 [stanley314]：使用 ping 命令根本无法 ping 通。

11、产生此问题的原因是：**BGP 选路规则：当两条路由度量均相等时，而且都来自于相同自治系统的 iBGP 的邻居，会优先选择 route id 较的 iBGP 邻居的路由。**

12、配置一个较高的 router id 给 R2 路由器解决此问题：

```
R2(config)#router bgp 64513
R2(config-router)#bgp router-id 172.16.255.254
```

批注 [stanley315]：给 R2 路由器配置较高的 route-id。以影响路由的选择。

13、在等邻居重新建立后，再次观察 R4 的路由表：

```
R4#show ip route

     10.0.0.0/30 is subnetted, 4 subnets
B       10.1.255.4 [200/0] via 10.1.255.9, 00:02:28
B       10.1.255.0 [200/0] via 10.1.255.5, 00:00:11
C       10.1.255.12 is directly connected, Serial1/1
C       10.1.255.8 is directly connected, Serial1/0
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [200/0] via 10.1.255.1, 00:00:01
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 10.1.255.14, 00:27:36
R4#
R4#ping 10.1.255.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.255.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/156/208 ms
R4#
```

批注 [stanley316]：查看 R4 的路由表，可以看出，此时 R4 已经学习到完整的路由表。

14、在 R2、R3 和 R4 上配置 OSPF 路由协议并开启同步规则，配置如下：

```
R2(config)#router bgp 64513
R2(config-router)#synchronization
R2(config-router)#exit
R2(config)#router ospf 1
R2(config-router)#network 10.1.255.0 0.0.0.3 area 0
R2(config-router)#network 10.1.255.4 0.0.0.3 area 0
```

批注 [stanley317]：开启 BGP 的同步规则。

```
R3(config)#router bgp 64513
R3(config-router)#synchronization
R3(config-router)#exit
R3(config)#router ospf 1
R3(config-router)#network 10.1.255.4 0.0.0.3 area 0
R3(config-router)#network 10.1.255.8 0.0.0.3 area 0
```

```
R4(config)#router bgp 64513
R4(config-router)#synchronization
R4(config-router)#exit
```

```
R4(config)#router ospf 1
R4(config-router)#network 10.1.255.8 0.0.0.3 area 0
R4(config-router)#network 10.1.255.12 0.0.0.3 area 0
```

15、查看 R1 路由器，确认是否学习到 150.150.1.0/24 网络路由：

```
R1#show ip route

     10.0.0.0/30 is subnetted, 4 subnets
B       10.1.255.4 [20/0] via 10.1.255.2, 00:21:11
C       10.1.255.0 is directly connected, Serial1/1
B       10.1.255.12 [20/0] via 10.1.255.2, 00:03:37
B       10.1.255.8 [20/0] via 10.1.255.2, 00:12:37
     130.130.0.0/24 is subnetted, 1 subnets
C       130.130.1.0 is directly connected, Loopback0
```

可以看出 R1 仍然没有学习到 150.150.1.0/24 网络路由。

16、查看 R2 路由表，可以其也无法学习到整个网络的路由：

```
R2#show ip route

     10.0.0.0/30 is subnetted, 4 subnets
O       10.1.255.4 [110/128] via 10.1.255.9, 00:00:44, Serial1/0
O       10.1.255.0 [110/192] via 10.1.255.9, 00:00:44, Serial1/0
C       10.1.255.12 is directly connected, Serial1/1
C       10.1.255.8 is directly connected, Serial1/0
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 10.1.255.14, 00:45:28
```

17、查看 R2 的 BGP 表：

```
R2#show ip bgp
   Network          Next Hop            Metric LocPrf Weight Path
*  10.1.255.0/30    10.1.255.1               0             0 64512 i
*>                  0.0.0.0                  0         32768 i
*> 10.1.255.4/30    0.0.0.0                  0         32768 i
* i                 10.1.255.6               0    100      0 i
r i10.1.255.8/30    10.1.255.10              0    100      0 i
r>i                 10.1.255.6               0    100      0 i
r>i10.1.255.12/30   10.1.255.10              0    100      0 i
*> 130.130.1.0/24   10.1.255.1               0             0 64512 i
* i150.150.1.0/24   10.1.255.14              0    100      0 64514 i
R2#
```

批注 [stanley318]： 此时指出 R2 的 BGP 已经学习到网络的路由，但由于未知的原因，导致此路由无法被使用。

18、查看详细的 150.150.1.0/24 网络路由描述：

```
R2#show ip bgp 150.150.1.0
BGP routing table entry for 150.150.1.0/24, version 0
Paths: (1 available, no best path)
```

```
  Not advertised to any peer
  64514
    10.1.255.14 (inaccessible) from 10.1.255.10 (10.1.255.13)
      Origin IGP, metric 0, localpref 100, valid, internal, not synchronized
```

批注 [stanley319]：此条路由被置为**不通告**状态。所以 R1 无法学习到此路由。

批注 [stanley320]：路由不同步。

19、产生此问题的主要原因是：**BGP 同步规则，不使用或不通告给任何 EBGP 邻居从 IBGP 邻居学习到路由，直到 IGPs 也学习到相同路由。**

20、使用路由重发布解决该问题，在 R4 上配置重发布：

```
R4(config)#router ospf 1
R4(config-router)#redistribute bgp 64513 metric 200 subnets
R4(config-router)#exit
```

批注 [stanley321]：重发布 BGP 的路由到 OSPF 协议中。

21、再次在 R2 上查看 150.150.1.0/24 网络路由的 BGP 描述：

```
R2#show ip bgp 150.150.1.0
BGP routing table entry for 150.150.1.0/24, version 16
Paths: (1 available, best #1, table Default-IP-Routing-Table, RIB-failure(17))
Flag: 0x820
  Advertised to non peer-group peers:
  10.1.255.1
  64514
    10.1.255.14 (metric 192) from 10.1.255.10 (10.1.255.13)
      Origin IGP, metric 0, localpref 100, valid, internal, synchronized, best
```

批注 [stanley322]：此时路由已同步，并且认为是最佳路由。

22、查看 R1 的路由表，确认路由：

```
R1#show ip route



     10.0.0.0/30 is subnetted, 4 subnets
B       10.1.255.4 [20/0] via 10.1.255.2, 00:25:11
C       10.1.255.0 is directly connected, Serial1/1
B       10.1.255.12 [20/0] via 10.1.255.2, 00:07:37
B       10.1.255.8 [20/0] via 10.1.255.2, 00:16:37
     130.130.0.0/24 is subnetted, 1 subnets
C       130.130.1.0 is directly connected, Loopback0
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 10.1.255.2, 00:01:36
R1#
```

23、同样，在 R2 上也需要配置重发布，来解决 R4 BGP 学习的 130.130.1.0/24 网络同步问题。具体配置不再列出。

24、实验完成。

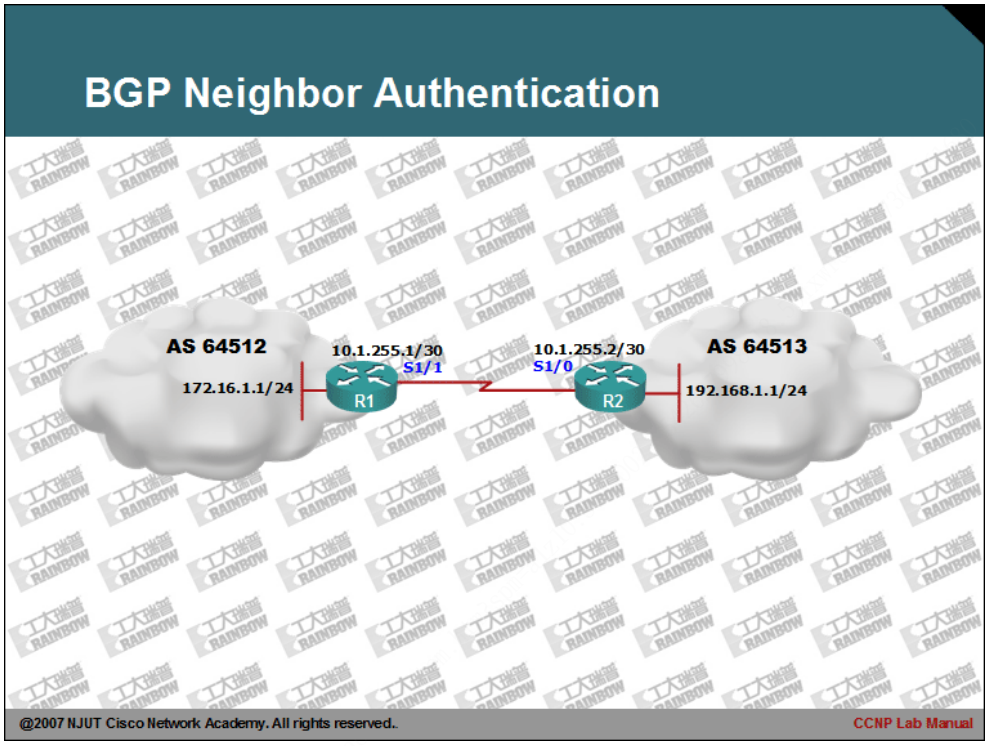
CCNP Lab Manual

Lab 33. BGP Neighbor Authentication

实验目的：

1、掌握其于 MD5 的 BGP 对等体认证配置。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置 R1 和 R2 的 BGP 协议

3、查看 R1 和 R2 的路由表。

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/1
B    192.168.1.0/24 [20/0] via 10.1.255.2, 00:32:23
R1#
```

```
R2#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 10.1.255.1, 00:33:19
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
R2#
```

4、配置 R1 路由器的 BGP 认证。

```
R1(config)#router bgp 64512
R1(config-router)#neighbor 10.1.255.2 password cisco123
```

批注 [stanley323]：指定与 10.1.255.2 的邻居 BGP 路由器建立会话需要使用密钥值为:cisco123

5、在配置完 R1 的 BGP 认证，IOS 会直接提示如下信息：

```
*Jun  9 15:48:03.323: %TCP-6-BADAUTH: No MD5 digest from 10.1.255.2(44020) to 10.1.255.1(179)
*Jun  9 15:48:05.143: %TCP-6-BADAUTH: No MD5 digest from 10.1.255.2(44020) to 10.1.255.1(179)
*Jun  9 15:48:13.263: %TCP-6-BADAUTH: No MD5 digest from 10.1.255.2(44020) to 10.1.255.1(179)
*Jun  9 15:48:15.343: %TCP-6-BADAUTH: No MD5 digest from 10.1.255.2(44020) to 10.1.255.1(179)
```

批注 [stanley324]：10.1.255.2 路由器使用其 TCP 的源端口 44020 与本地 TCP 的端口 179 建立 BGP 会话时，没有携带 MD5 密钥认证不通过。

6、查看 R1 和 R2 的路由表以及 BGP 的数据库，此时 R1 和 R2 路由器 BGP 协议，已经释放了原先学习到的 BGP 的网络路由。

```
R1#show ip route
```

```
Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/1
R1#
R1#show ip bgp
BGP table version is 4, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
R1#
```

```
R2#show ip route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
R2#
R2#show ip bgp
BGP table version is 4, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      0.0.0.0                  0         32768 i
R2#
```

7、查看 R2 的汇总信息。

```
R2#show ip bgp summary
......
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 209 total bytes of memory
BGP activity 2/1 prefixes, 2/1 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
```

```
10.1.255.1      4 64512      43      42        0    0    0 00:04:00 Active
R2#
```

批注 [stanley325]：由于认证不通过，所以无法建立对等体关系。

8、配置 R2 的 BGP 的认证密码。

```
R2(config)#router bgp 64513
R2(config-router)#neighbor 10.1.255.1 password cisco123
R2(config-router)#exit
```

9、当在 R2 上配置完 BGP 的认证密码后，R1 或是 R2 路由器 IOS 提示如下信息。

```
*Jun  9 15:54:47.559: %TCP-6-BADAUTH: No MD5 digest from 10.1.255.2(16055) to 10.1.255.1(179)
*Jun  9 15:56:51.859: %BGP-5-ADJCHANGE: neighbor 10.1.255.2 Up
```

批注 [stanley326]：此条表明，BGP 认证通过。

10、查看 BGP 的汇总信息。

```
R1#show ip bgp summary
BGP router identifier 172.16.1.1, local AS number 64512
BGP table version is 5, main routing table version 5
2 network entries using 202 bytes of memory
2 path entries using 96 bytes of memory
2 BGP path attribute entries using 120 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 442 total bytes of memory
BGP activity 3/1 prefixes, 3/1 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.255.2      4 64513      45      49        5    0    0 00:01:33        1
R1#
```

11、查看 R1 路由器的路由表，此时 R1 路由器已经学习到 AS 64513 自治系统路由。

```
R1#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/1
B    192.168.1.0/24 [20/0] via 10.1.255.2, 00:03:28
R1#
```

12、查看 R2 路由器的路由表。

```
R2#show ip route
```

```
Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 10.1.255.1, 00:04:26
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
C    192.168.1.0/24 is directly connected, Loopback0
R2#
```

13、实验完成。

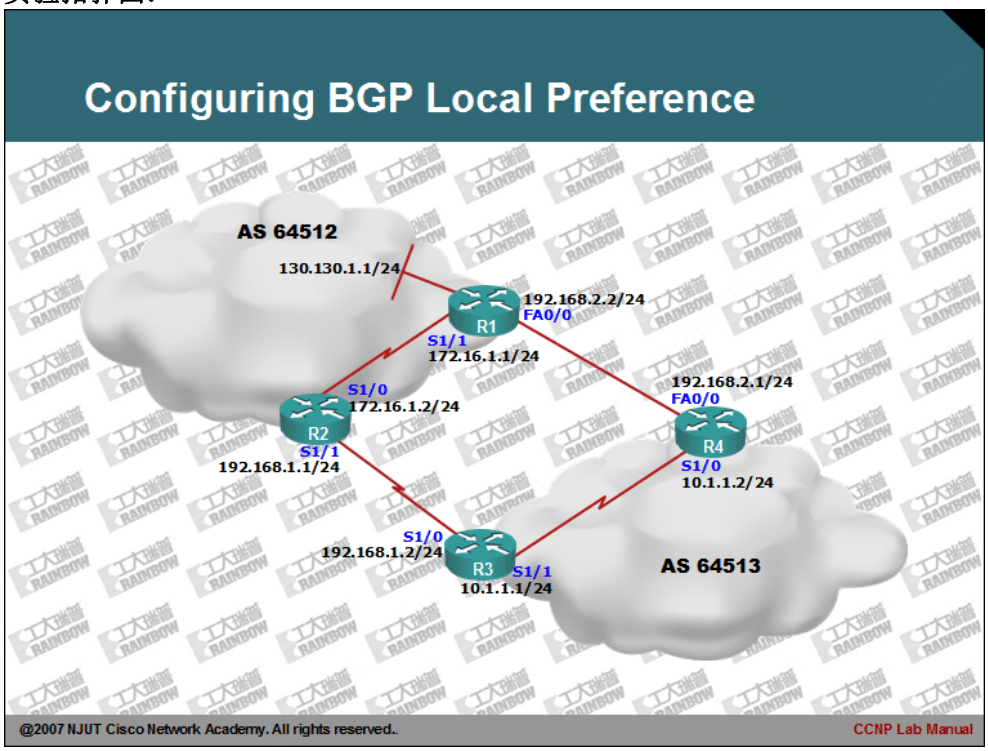
CCNP Lab Manual

Lab 34. Configuring BGP Local Preference

实验目的：

1、理解掌握 BGP 的本地优选属性概念和配置方法。
2、本地优选的属性默认值为 100，较高值的路径会被优先选择。
3、本地优先属性，决定离开本自治系统最佳的路径。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置所有的路由器的 BGP 协议。由于 BGP 收敛速度较慢，当配置好 BGP 后，需要等待一段时间。

3、查看 R3 的路由表。

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.1.1, 00:01:06
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/1
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 192.168.1.1, 00:01:06
C    192.168.1.0/24 is directly connected, Serial1/0
B    192.168.2.0/24 [200/0] via 10.1.1.2, 00:00:11
R3#
```

批注 [stanley327]: R3 到达 130.130.1.0/24 的网络下一跳是 192.168.1.1。

4、查看 R4 的路由表。

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.2.2, 00:02:18
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/0
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 192.168.2.2, 00:02:18
B    192.168.1.0/24 [200/0] via 10.1.1.1, 00:02:18
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R4#
```

批注 [stanley328]: R4 到达 130.130.1.0/24 的网络下跳是 192.168.2.2。

5、理论上 BGP 选择的都是最佳路由。但是对拓扑仔细观察。R4 与 R1 之间快速以太网，而且其速度是 100MB，而 R3 目前选择到达 130.130.1.0/24 的网络下一跳是 192.168.1.1。其需要通过 2 条广域网的串口链路。如果假设串口链路的速度是 2MB 的 DDN 专线。则 R3 选择次佳的路由。**其主要原因是，BGP 在选择最佳路由时，并不会考具体链路的带宽。为了解决这一问题，可以在本地配置“本**

地优先”来确定数据流如何流出本自治系统。

6、查看 R3 的 BGP 数据库信息表。

```
R3#show ip bgp

BGP table version is 7, local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i10.1.1.0/24     10.1.1.2                 0    100      0 i
*>                 0.0.0.0                  0         32768 i
* i130.130.1.0/24  192.168.2.2              0    100      0 64512 i
*>                 192.168.1.1                           0 64512 i
* i172.16.1.0/24   192.168.2.2              0    100      0 64512 i
*>                 192.168.1.1              0             0 64512 i
*> 192.168.1.0     0.0.0.0                  0         32768 i
*                  192.168.1.1              0             0 64512 i
*>i192.168.2.0     10.1.1.2                 0    100      0 i
*                  192.168.1.1                           0 64512 i
R3#
```

批注 [stanley329]: 其中的加粗显示的 100 为默认的本地优先属性值。

7、查看 R4 的 BGP 的数据库信息表。

```
R4#show ip bgp

BGP table version is 9, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i10.1.1.0/24     10.1.1.1                 0    100      0 i
*>                 0.0.0.0                  0         32768 i
* i130.130.1.0/24  192.168.1.1              0    100      0 64512 i
*>                 192.168.2.2              0             0 64512 i
* i172.16.1.0/24   192.168.1.1              0    100      0 64512 i
*>                 192.168.2.2              0             0 64512 i
*>i192.168.1.0     10.1.1.1                 0    100      0 i
*                  192.168.2.2                           0 64512 i
*> 192.168.2.0     0.0.0.0                  0         32768 i
*                  192.168.2.2              0             0 64512 i
R4#
```

8、通过对比 R3 与 R4 路由器的 BGP 数据库，只需要调整 R4 路由器所学习的所有

BGP 路由的本地优先值。**因为 BGP 会优先选择本地优先属性值较高的路由。**

9、配置 R4 的路由器，调整本地优先属性值为 200。

```
R4(config)#router bgp 64513
R4(config-router)#bgp default local-preference 200
R4(config-router)#exit
R4(config)#
```

批注 [stanley330]：调整，BGP 的默认的本地优先属性值为 200。

10、查看 R3 的 BGP 数据库。

```
R3#show ip bgp

BGP table version is 10, local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i10.1.1.0/24     10.1.1.2                 0    200      0 i
*>                 0.0.0.0                  0         32768 i
*>i130.130.1.0/24  192.168.2.2              0    200      0 64512 i
*                  192.168.1.1                           0 64512 i
*>i172.16.1.0/24   192.168.2.2              0    200      0 64512 i
*                  192.168.1.1              0             0 64512 i
* i192.168.1.0     192.168.2.2              0    200      0 64512 i
*>                 0.0.0.0                  0         32768 i
*                  192.168.1.1              0             0 64512 i
*>i192.168.2.0     10.1.1.2                 0    200      0 i
*                  192.168.1.1                           0 64512 i
R3#
```

批注 [stanley331]：当对 R4 的本地优先属性进行调整后，在 R3 上会发现从 R4 学习到的路由的本地优先已经改变 200。

同时，也可以看出，此时，R3 到达 130.130.1.0/24 的子网，其下一跳为 192.168.2.2，为最佳路由。

11、再次查看 R3 的路由表

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [200/0] via 192.168.2.2, 00:06:41
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/1
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [200/0] via 192.168.2.2, 00:06:41
C    192.168.1.0/24 is directly connected, Serial1/0
B    192.168.2.0/24 [200/0] via 10.1.1.2, 00:26:51
R3#
```

批注 [stanley332]：到达 130.130.1.0/24 子网，其下一跳为 192.168.2.2/24。

12、在 R3 上到达 130.130.1.0/24 的子网下一跳为 192.168.2.2，是因为 **BGP 在向 IBGP 对等体通告路由时，其下一跳不变，这种机制被称为 BGP 的下一跳属性。**

为了能够在 R3 上真实反应路由变化，可以在 R4 上配置通告给 R3 的路由，其下一跳强制为 R4 自己。配置如下：

```
R4(config)#router bgp 64513
R4(config-router)#neighbor 10.1.1.1 next-hop-self
```

批注 [stanley333]: 向 10.1.1.1 的对等体发送路由。会主动将下一跳设 R4 自己。

13、再次查看 R3 的路由表，确认配置。

```
R3#show ip route

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [200/0] via 10.1.1.2, 00:01:32
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/1
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [200/0] via 10.1.1.2, 00:01:32
C    192.168.1.0/24 is directly connected, Serial1/0
B    192.168.2.0/24 [200/0] via 10.1.1.2, 00:32:58
R3#
```

批注 [stanley334]: 此时，下一跳为 10.1.1.2。

14、使用 traceroute 命令跟踪路由信息。

```
R3#traceroute 130.130.1.1

Type escape sequence to abort.
Tracing the route to 130.130.1.1

  1 10.1.1.2 92 msec 72 msec 72 msec
  2 192.168.2.2 212 msec *  120 msec
R3#
```

15、使用 PING 命令确认路由有效性。

```
R3#ping 130.130.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.130.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/130/168 ms
R3#
```

16、实验完成。

CCNP Lab Manual

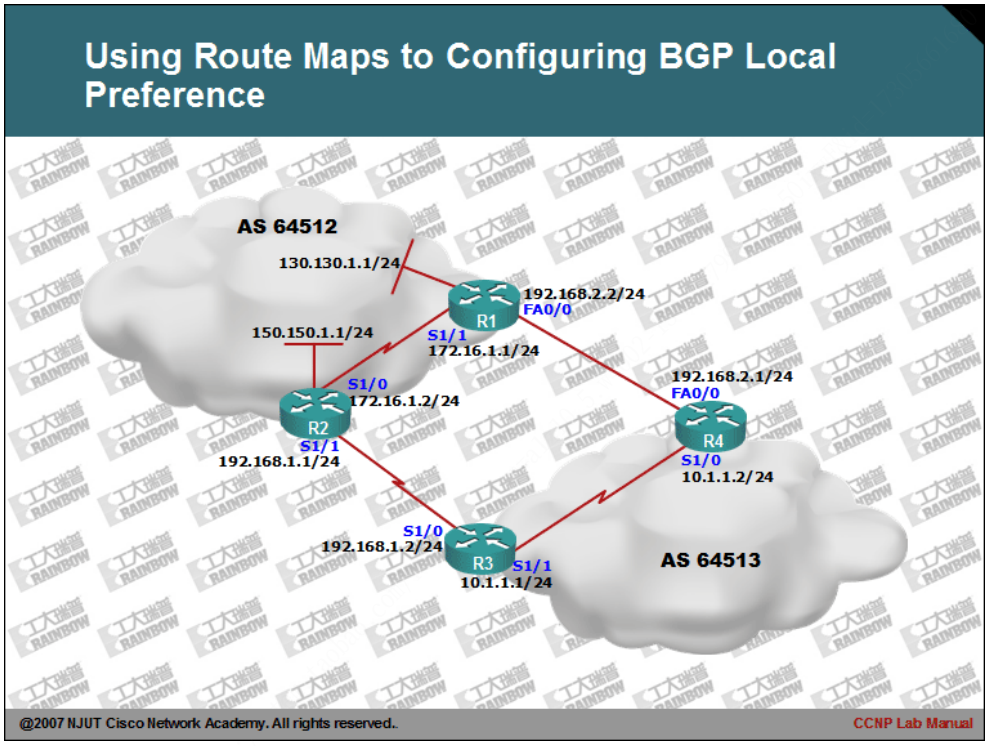
Lab 35. Using Route Maps to Configuring BGP Local Preference

实验目的：

1、掌握基于 route-map 的本地优先配置方法。

2、使用 route-map 配置可以定置基于目标网络的本地优先。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置各台路由器的 BGP 协议。

3、查看 R3 与 R4 的路由表。

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.1.1, 00:04:30
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/1
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 192.168.1.1, 00:04:30
C    192.168.1.0/24 is directly connected, Serial1/0
B    192.168.2.0/24 [200/0] via 10.1.1.2, 00:06:07
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.1.1, 00:04:30
R3#
```

批注 [stanley335]: 到达 130.130.1.0/24 下一跳为 192.168.1.1

批注 [stanley336]: 到达 150.150.1.0/24 下一跳为 192.168.1.1

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.2.2, 00:06:14
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/0
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 192.168.2.2, 00:06:14
B    192.168.1.0/24 [200/0] via 10.1.1.1, 00:07:42
C    192.168.2.0/24 is directly connected, FastEthernet0/0
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.2.2, 00:05:45
R4#
```

批注 [stanley337]: 到达 130.130.1.0/24 下一跳为 192.168.2.2

批注 [stanley338]: 到达 150.150.1.0/24 下一跳为 192.168.2.2

4、对 R3 与 R4 的路由表进行分析结果如下表，假设 serial 链路为 2Mb 专线：

```
     serial       loopback
R3 --------> R2 ----------> 150.150.1.0/24

     serial        serial       loopback
R3 --------> R2 --------> R1 -----------> 150.150.1.0/24

    fastEth       loopback
R4 --------> R1 -----------> 150.150.1.0/24

    fastEth       serial       loopback
R4 --------> R1 --------> R2 -----------> 150.150.1.0/24
```

通过上述分析及结合拓扑，可以得出 R3 到达 130.130.1.0/24 的网络最佳路由为

```
      serial       fastEth       loopback
 R3 --------> R4 --------> R1 -----------> 150.150.1.0/24
```

为了配置 BGP 协议能够为 R3 选择最佳路由到达 150.150.1.0/24 的网络，可以使用本地优先属性。但是如果仅仅简单的配置在 R3 的本地优先为 100，R4 的本地优先为 200，那么又会产生另外一个问题，即 R3 如果需要到达 150.150.1.0/24 的网络，会选择如下路由：

```
     serial       fastEth       serial       loopback
 R3 --------> R4 --------> R1 -------> R2 ----------->130.130.1.0/24
```

生产此问题的主要原因是：本地优先会影响数据流如何流出本地自治系统。

解决问题的方法是：使用基于 route-map 的策略配置，针对不同的目标进行路由调整。

5、首先查看 R3 和 R4 路由器的数据库：

```
R3#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.............
*> 130.130.1.0/24   192.168.1.1                           0 64512 i
* i                 192.168.2.2              0    100      0 64512 i
* i150.150.1.0/24   192.168.2.2              0    100      0 64512 i
*>                  192.168.1.1              0             0 64512 i
.............
R3#
```

R3 路由器的 BGP 协议没有选择 192.168.2.2/24 的原因是因为 **BGP 的选路规则：**

EBGP 对等体通告的路由优于 IBGP 对等体通告的路由。

```
R4#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.............
* i130.130.1.0/24    192.168.1.1              0    100      0 64512 i
*>                   192.168.2.2              0             0 64512 i
*> 150.150.1.0/24    192.168.2.2                            0 64512 i
* i                  192.168.1.1              0    100      0 64512 i
.............
R4#
```

6、由于 BGP 的本地优先默认值为 100，所以在 R4 上只需要将针对 130.130.1.0/24 网络路由的本地优先调整大于 100 即可，其配置如下：

```
R4(config)#access-list 1 permit 130.130.1.0 0.0.0.255
R4(config)#
R4(config)#route-map set_lp permit 10
R4(config-route-map)#match ip address 1
R4(config-route-map)#set local-preference 200
R4(config-route-map)#exit
R4(config)#
R4(config)#route-map set_lp permit 20
R4(config-route-map)#exit
R4(config)#
R4(config)#router bgp 64513
R4(config-router)#neighbor 192.168.2.2 route-map set_lp in
R4(config-router)#exit
R4(config)#exit
R4#
R4#clear ip bgp * soft in
R4#
```

批注 [stanley339]：使用 ACL 匹配需要修改本地优先的路由。

批注 [stanley340]：对 ACL 1 所指出的路由进行匹配

批注 [stanley341]：对匹配 ACL 1 所指出的路由，修改其本地优先值为 200，此值将会影响本地自治系统的其它路由器，如何到达 130.130.1.0/24 的网络。

批注 [stanley342]：配置空的路由图，保证其它路由均按默认方式进行通告。

批注 [stanley343]：针对 192.168.2.2 的对等体发送的路由进行操作。其方向是 in 的方向。

批注 [stanley344]：刷新入站的策略配置，加快 BGP 的收敛。

7、在 R4 上查看 BGP 的数据库。

```
R4#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.............
*> 130.130.1.0/24    192.168.2.2              0    200      0 64512 i
*> 150.150.1.0/24    192.168.2.2                            0 64512 i
* i                  192.168.1.1              0    100      0 64512 i
.............
R4#
```

批注 [stanley345]：R4 上显示相应的路由的本地优先已经为 200。

8、查看 R3 的 BGP 的数据库。

```
R3#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.............
*  130.130.1.0/24   192.168.1.1                             0 64512 i
*>i                 192.168.2.2              0    200      0 64512 i
* i150.150.1.0/24   192.168.2.2              0    100      0 64512 i
*>                  192.168.1.1              0             0 64512 i
.............
R3#
```

批注 [stanley346]：此时，在R3上查看到达目标网络的路由的本地优先为200，其下一跳192.168.2.2。

9、为了确切的判断出R3到达130.130.1.0/24的网络路由，使用的是最佳路由，在R4路由器上配置下一跳属性。

```
R4(config)#router bgp 64513
R4(config-router)#neighbor 10.1.1.1 next-hop-self
R4(config-router)#exit
```

批注 [stanley347]：配置发向R3的路由其下一跳为R4路由器自己。

10、再次查看R3的BGP数据库。

```
R3#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.............
*  130.130.1.0/24   192.168.1.1                             0 64512 i
*>i                 10.1.1.2                 0    200      0 64512 i
* i150.150.1.0/24   10.1.1.2                 0    100      0 64512 i
*>                  192.168.1.1              0             0 64512 i
.............
R3#
```

批注 [stanley348]：此时已经能够直接判断出，R3到达130.130.1.0/24网络下一跳是10.1.1.2。

11、查看R3和R4的路由表，可以看出本地优先仅仅影响了64513自治系统的所有路由器如何到达130.130.1.0/24的网络，没有影响到其它的目标路由。

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.1.1, 00:54:00
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/1
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [200/0] via 10.1.1.2, 00:02:46
C    192.168.1.0/24 is directly connected, Serial1/0
B    192.168.2.0/24 [200/0] via 10.1.1.2, 00:55:37
     150.150.0.0/24 is subnetted, 1 subnets
```

```
B       150.150.1.0 [20/0] via 192.168.1.1, 00:54:00
R3#
```

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.2.2, 00:10:58
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/0
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 192.168.2.2, 00:55:38
B    192.168.1.0/24 [200/0] via 10.1.1.1, 00:57:06
C    192.168.2.0/24 is directly connected, FastEthernet0/0
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.2.2, 00:10:58
R4#
```

12、使用 tracert 命令确认路由信息：

```
R3#traceroute 130.130.1.1

Type escape sequence to abort.
Tracing the route to 130.130.1.1

  1 10.1.1.2 16 msec 48 msec 80 msec
  2 192.168.2.2 96 msec *  80 msec

R3#
R3#traceroute 150.150.1.1

Type escape sequence to abort.
Tracing the route to 150.150.1.1

  1 192.168.1.1 40 msec *  24 msec

R3#
```

17、实验完成。

CCNP Lab Manual

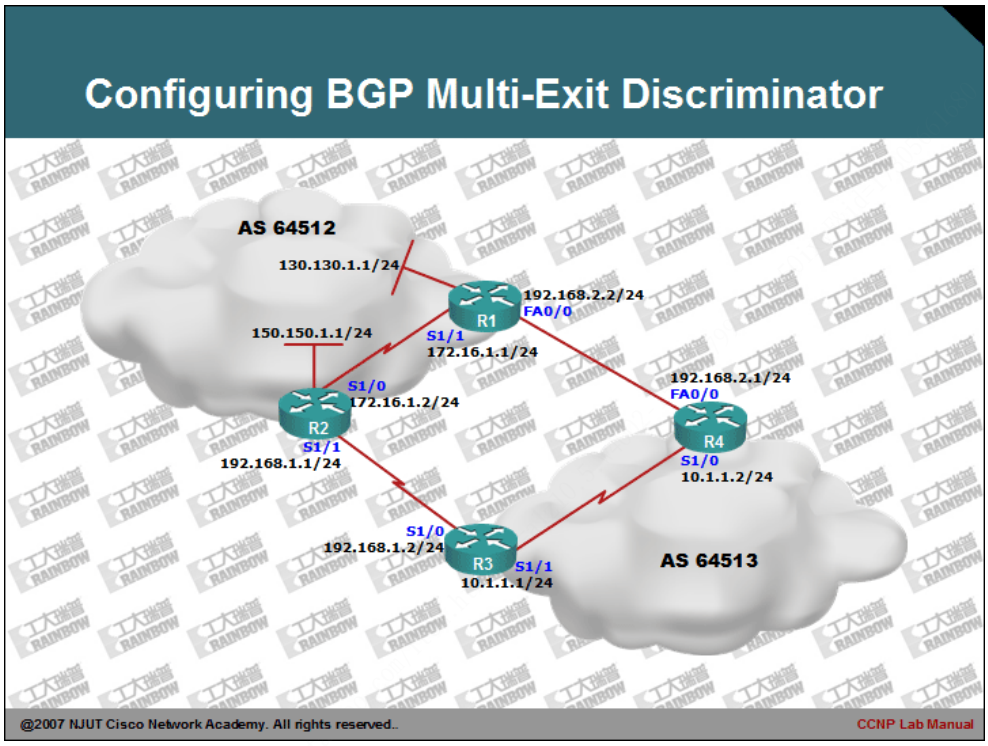
Lab 36. Configuring BGP Multi-Exit Discriminator

实验目的：

1、理解 MED 属性能够影响,其它的自治系统的数据流如何流入本地自治系统。

2、掌握基于 route-map 的 MED 配置方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置各台路由器的 BGP 协议。

3、在前一个实验 **Using Route Maps to Configuring BGP Local Preference** 中，介绍如何使用本地优先配置数据流如何流出本地自治系统。在本实验中，会使用另一个 BGP 的的属性即 MED 属性配置，影响其它自治系统数据流流入本地自治系统。

4、查看 R3 和 R4 的路由表，本次实验仍然关注 64512 自治系统中的两个环回接口路由：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.1.1, 00:08:58
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/1
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 192.168.1.1, 00:08:58
C    192.168.1.0/24 is directly connected, Serial1/0
B    192.168.2.0/24 [200/0] via 10.1.1.2, 00:08:58
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.1.1, 00:08:58
R3#
```

```
R4#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.2.2, 00:20:47
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/0
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/0] via 192.168.2.2, 00:20:47
B    192.168.1.0/24 [200/0] via 10.1.1.1, 00:13:52
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.2.2, 00:19:48
R4#
```

5、根据路由表可以看出，R3 路由器到达 R1 的 130.130.1.0/24 子网，选择了一条次佳的路由。在实际网络应用中，可能由于 R3 的将到达 AS 64512 自治的流量通过其直连接口，直接发送给 R2 路由器，而 R3 与 R2 之间的链路是一条低速的 WAN 链路，因此会导致其接口会产生拥塞现象。因此，64512 自治系统更希望 R3 能够充分使用 R4 与 R1 之间的快速以太网链路来进行数据的传输。为了实现这一目的，可以在 R1 与 R2 上配置 MED 属性，因为 **MED 属性可以实现：影响其它的自治系统的数据流，如何流入本地自治系统。**

6、**根据 MED 的属性值越低的哪条路由，会被优先选择的特性。而且 MED 值默认为 0**。因此，可以在 R2 上配置其向 R2 通告的 130.130.1.0/24 的网络路由的 MED 值高于默认值即可。如果不主动修改 R1 的 MED 默认值的话。

7、为了能够观察到 MED 的配置前后路由变化，需要先查看 R3 与 R4 的 BGP 数据库表：

```
R3#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.........
*> 130.130.1.0/24   192.168.1.1                            0 64512 i
* i                 192.168.2.2              0    100      0 64512 i
*> 150.150.1.0/24   192.168.1.1              0             0 64512 i
* i                 192.168.2.2              0    100      0 64512 i
.........
R3#
```

```
R4#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.........
* i130.130.1.0/24   192.168.1.1              0    100      0 64512 i
*>                  192.168.2.2              0             0 64512 i
* i150.150.1.0/24   192.168.1.1              0    100      0 64512 i
*>                  192.168.2.2                            0 64512 i
```

```
.........
R4#
```

7、在 R2 上实施 MED 的策略配置。

```
R2(config)#access-list 1 permit 130.130.1.0 0.0.0.255
R2(config)#
R2(config)#route-map set_med permit 10
R2(config-route-map)#match ip address 1
R2(config-route-map)#set metric 100
R2(config-route-map)#exit
R2(config)#
R2(config)#route-map set_med permit 20
R2(config-route-map)#exit
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 192.168.1.2 route-map set_med out
R2(config-router)#exit
R2(config)#
R2#
R2#clear ip bgp * soft out
R2#
```

批注 [stanley349]：使用 ACL 指出需要修改的 MED 的路由。

批注 [stanley350]：用于匹配查询 ACL 1 所指出的路由条目。

批注 [stanley351]：对于匹配成功的路由条目，将其 MED 值设为 100

批注 [stanley352]：配置对于其它的路由采用默认的方式进行宣告。即不做任何修改。

批注 [stanley353]：针对对等体 192.168.1.2 进行策略路由。

方向 out，是指出从 R2 向 R1 发出的路由进行策略设置。

8、查看 R3 与 R4 的 BGP 数据库信息。

```
R3#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.........
*  130.130.1.0/24   192.168.1.1              100             0 64512 i
*>i                 192.168.2.2                0    100      0 64512 i
*> 150.150.1.0/24   192.168.1.1                0             0 64512 i
* i                 192.168.2.2                0    100      0 64512 i
.........
R3#
```

批注 [stanley354]：刷新外出的策略配置，用于加快 BGP 的收敛。

批注 [stanley355]：从 R2 通告的 130.130.1.0/24 网络路由的 MED 值为 100。

批注 [stanley356]：由于 BGP 会选择较低的 MED 值的路由，因此 R2 选择下一跳为 192.168.1.1。

```
R4#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.........
*> 130.130.1.0/24   192.168.2.2                0             0 64512 i
* i150.150.1.0/24   192.168.1.1                0    100      0 64512 i
*>                  192.168.2.2                               0 64512 i
.........
R4#
```

批注 [stanley357]：由于 MED 属性为不可传递，因此，其并没有影响到 R4 的 BGP 的路由协议。

9、为了确切的判断出 R3 到达 130.130.1.0/24 的网络路由，使用的是最佳路由，在 R4 路由器上配置下一跳属性。配置如下：

```
R4(config)#router bgp 64513
R4(config-router)#neighbor 10.1.1.1 next-hop-self
R4(config-router)#exit
R4(config)#exit
```

10、在 R3 路由器上查看 BGP 的数据库和路由表。

```
R3#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
.........
*  130.130.1.0/24   192.168.1.1              100             0 64512 i
*>i                 10.1.1.2                   0    100      0 64512 i
*> 150.150.1.0/24   192.168.1.1                0             0 64512 i
* i                 10.1.1.2                   0    100      0 64512 i
.........
R3#
```

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.1.1, 00:48:49
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial1/1
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [200/0] via 10.1.1.2, 00:03:50
C    192.168.1.0/24 is directly connected, Serial1/0
B    192.168.2.0/24 [200/0] via 10.1.1.2, 00:48:49
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.1.1, 00:48:49
R3#
```

11、使用 tracert 命令确认路由信息：

```
R3#traceroute 130.130.1.1

Type escape sequence to abort.
Tracing the route to 130.130.1.1

  1 10.1.1.2 32 msec 64 msec 80 msec
  2 192.168.2.2 128 msec *  84 msec
```

```
R3#
```

12、实验完成。

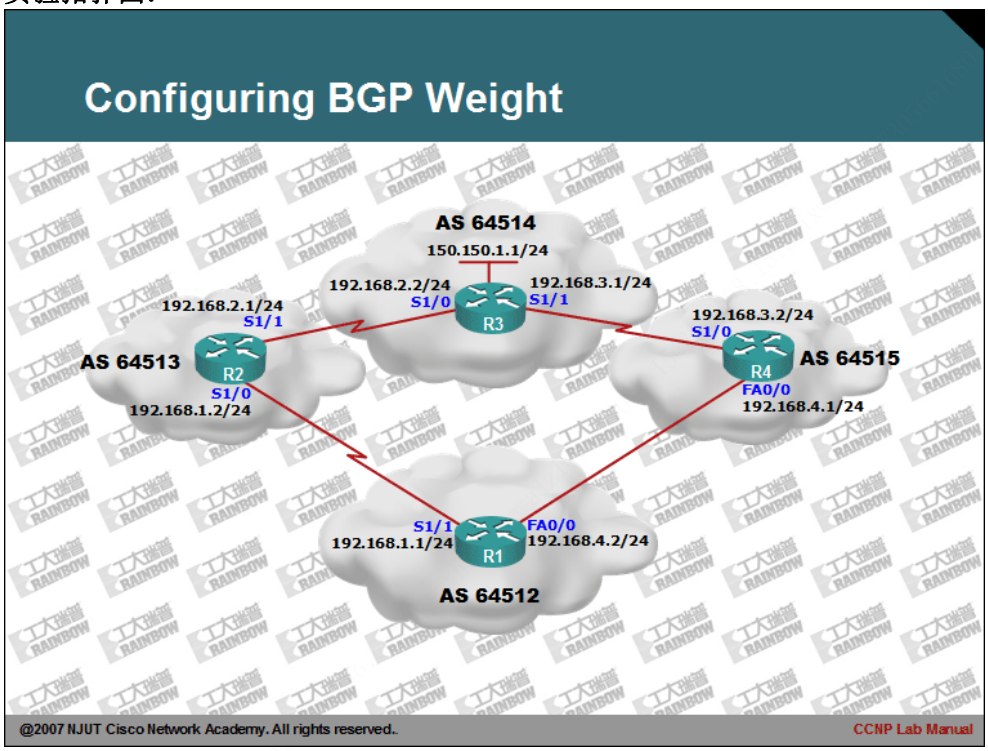
Lab 37. Configuring BGP Weight

实验目的：

1、当本地出口路由器,有多条外出自治系统的链路时,应用权重(Weight)属性能够决定数据流从本地路由器哪条出口链路流出本地自治系统.

2、权重(Weight)属性为 Cisco 私有属性。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置各台路由器的 BGP 协议，并使用 show ip bgp 确认协议能够正常的工作。建议 BGP 配置顺序为 R1、R2、R3、R4。以方便于实验。强调配置 BGP 的顺序，主要是因为，在本实验中 R1 到达 150.150.1.0/24 网络的两条路径，在 BGP 协议中，会认为两条路径是等价的，但是 BGP 又不是用于均分负载的实验，因此，BGP 会优先选择从 R1 到达目标。其原因是 **BGP 的选路规则：1、最先收到路由优先于后收到的路由。2、优先选择 BGP 的 Router-ID 较低的路由。**

3、查看 R1 的路由表：

```
R1#show ip route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial1/1
B    192.168.2.0/24 [20/0] via 192.168.1.2, 00:16:39
B    192.168.3.0/24 [20/0] via 192.168.4.1, 00:16:25
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.1.2, 00:16:39
R1#
```

批注 [stanley358]： 到达 150.150.1.0/24 网络的下一跳为 192.168.1.2。

4、查看 R1 的 BGP 数据表：

```
R1#show ip bgp
BGP table version is 7, local router ID is 192.168.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  150.150.1.0/24   192.168.4.1                             0 64515 64514 i
*>                  192.168.1.2                             0 64513 64514 i
*  192.168.1.0      192.168.1.2              0              0 64513 i
*>                  0.0.0.0                  0          32768 i
*  192.168.2.0      192.168.4.1                             0 64515 64514 i
*>                  192.168.1.2              0              0 64513 i
*> 192.168.3.0      192.168.4.1              0              0 64515 i
*                   192.168.1.2                             0 64513 64514 i
*  192.168.4.0      192.168.4.1              0              0 64515 i
```

批注 [stanley359]： 由于 R2 向 R1 通告的路由比 R4 向 R1 通告的路由较早，同时 R2 的 BGP 的 Router-ID 比 R4 的 Router-ID 要低，所以 R1 先择了 R2 的路由到达 150.150.1.0/24 网络。

```
*>                  0.0.0.0                  0         32768 i
R1#
```

5、查看 R1 的邻居表信息：

```
R1#show ip bgp neighbors
BGP neighbor is 192.168.1.2,  remote AS 64513, external link
  BGP version 4, remote router ID 192.168.2.1
  BGP state = Established, up for 02:10:56

.............

BGP neighbor is 192.168.4.1,  remote AS 64515, external link
  BGP version 4, remote router ID 192.168.4.1
  BGP state = Established, up for 02:09:04
R1#
```

批注 [stanley360]: BGP 的 Router-ID

6、通过拓扑可以看出，64512 的自治系统到达 150.150.1.0/24 的网络，其最佳路由是从自治系统 64514 通过，而不是 64513。因此，BGP 又一次的选择了一条次佳的路由。

7、在 R1 上配置权重属性，解决次佳路由选择的问题。配置如下：

```
R1(config)#router bgp 64512
R1(config-router)#neighbor 192.168.4.1 weight 100
R1(config-router)#neighbor 192.168.1.2 weight 50
R1(config-router)#exit
R1#clear ip bgp * soft
```

批注 [stanley361]: 指定 192.168.4.1 的邻居发送的路由权限为 100。

批注 [stanley362]: 指定 192.168.1.2 的邻居发送的路由权重为 50。
此条命令可以忽略不写。因此权重默认值为 0。

批注 [stanley363]: 刷新 BGP 的策略配置，加快 BGP 的收敛。

8、为了确认不同的权重值对路由的影响，查看 R1 路由表和 BGP 的数据库：

```
R1#show ip bgp

BGP table version is 13, local router ID is 192.168.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 150.150.1.0/24   192.168.4.1                          100 64515 64514 i
*                   192.168.1.2                           50 64513 64514 i
*  192.168.1.0      192.168.1.2              0            50 64513 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.2.0      192.168.4.1                          100 64515 64514 i
*                   192.168.1.2              0            50 64513 i
*> 192.168.3.0      192.168.4.1              0           100 64515 i
*                   192.168.1.2                           50 64513 64514 i
```

批注 [stanley364]: 由于 192.168.1.0/24 对于 R1 是直接连接的，所以其权重值默认为最大。以避免路由的环路。

```
*  192.168.4.0      192.168.4.1              0            100 64515 i
*>                  0.0.0.0                  0          32768 i
R1#
```

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial1/1
B    192.168.2.0/24 [20/0] via 192.168.4.1, 00:01:01
B    192.168.3.0/24 [20/0] via 192.168.4.1, 03:12:01
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.4.1, 00:01:01
R1#
```

批注 [stanley365]：此时 BGP 已经选择最佳的路由。

9、通过对 BGP 的数据库分析，可以看出，从 R2 路由器发送的路由，其权重均为 50，而从 R4 发送的路由的权重值均为 100。由于 **BGP 的选路规则：优先选择权重较高的路由。**因此 64512 的自治系统数据流流出本地自治系统时，均使用 R4 作为下一跳。但是又会生产另外一个问题，即 R1 到达 R2 的 192.168.2.0/24 的子网，使用 R4 是不智的行为。因为从 R4 到达 192.168.2.0/24 网络最佳路由是直接发送给 R2。而采用 neighbor *.*.*.* weight ***的配置方法本不是最完美的配置。为了解决这一问题，建议使用路由图的配置，针对目标网络设置不同的权重值

10、在 R1 上使用 route-map 配置权重值，配置如下：

```
R1(config)#router bgp 64512
R1(config-router)#no neighbor 192.168.1.2 weight 50
R1(config-router)#no neighbor 192.168.4.1 weight 100
R1(config-router)#exit
R1(config)#
R1(config)#access-list 1 permit 150.150.1.0 0.0.0.255
R1(config)#
```

批注 [stanley366]：配置 ACL 以便于路由图调用。

```
R1(config)#route-map set_weight permit 10
R1(config-route-map)#match ip address 1
R1(config-route-map)#set weight 100
R1(config-route-map)#exit
R1(config)#
R1(config)#
R1(config)#route-map set_weight permit 20
R1(config-route-map)#exit
R1(config)#
R1(config)#router bgp 64512
R1(config-router)#neighbor 192.168.4.1 route-map set_weight in
R1(config-router)#exit
R1(config)#exit
R1#clear ip bgp * soft
R1#
```

批注 [stanley367]： 如果路由匹配 ACL 1 ，则修改其权重为 100。

批注 [stanley368]： 针对 192.168.4.1 的邻居发送的路由进行策略设置。
其方向是 in，因为是对 R4 发送给本地路由。

批注 [stanley369]： 刷新 BGP 的策略配置，加快 BGP 的收敛。

11、查看 R1 的路由表：

```
R1#show ip route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial1/1
B    192.168.2.0/24 [20/0] via 192.168.1.2, 00:03:45
B    192.168.3.0/24 [20/0] via 192.168.4.1, 00:03:45
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.4.1, 00:00:00
R1#
```

批注 [stanley370]： 通过路由图的配置，仍然可以保证 BGP 选择最佳路由。

12、查看 R1 的 BGP 的数据库：

```
R1#show ip bgp
BGP table version is 21, local router ID is 192.168.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 150.150.1.0/24   192.168.4.1                       100 64515 64514 i
*                   192.168.1.2                         0 64513 64514 i
*  192.168.1.0      192.168.1.2              0          0 64513 i
*>                  0.0.0.0                  0      32768 i
*  192.168.2.0      192.168.4.1                         0 64515 64514 i
*>                  192.168.1.2              0          0 64513 i
*> 192.168.3.0      192.168.4.1              0          0 64515 i
```

批注 [stanley371]： 仅有被匹配的路由，其权重值才会被修改为 100。

```
*                  192.168.1.2                        0 64513 64514 i
*  192.168.4.0     192.168.4.1              0         0 64515 i
*>                 0.0.0.0                  0     32768 i
R1#
```

13、使用 ping 和 tracert 命令，确认路由有效性：

```
R1#ping 150.150.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.150.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/126/216 ms
R1#
R1#traceroute 150.150.1.1

Type escape sequence to abort.
Tracing the route to 150.150.1.1

  1 192.168.4.1 16 msec 60 msec 64 msec
  2 192.168.3.1 [AS 64515] 144 msec *  32 msec
R1#
```

14、实验完成。

CCNP Lab Manual

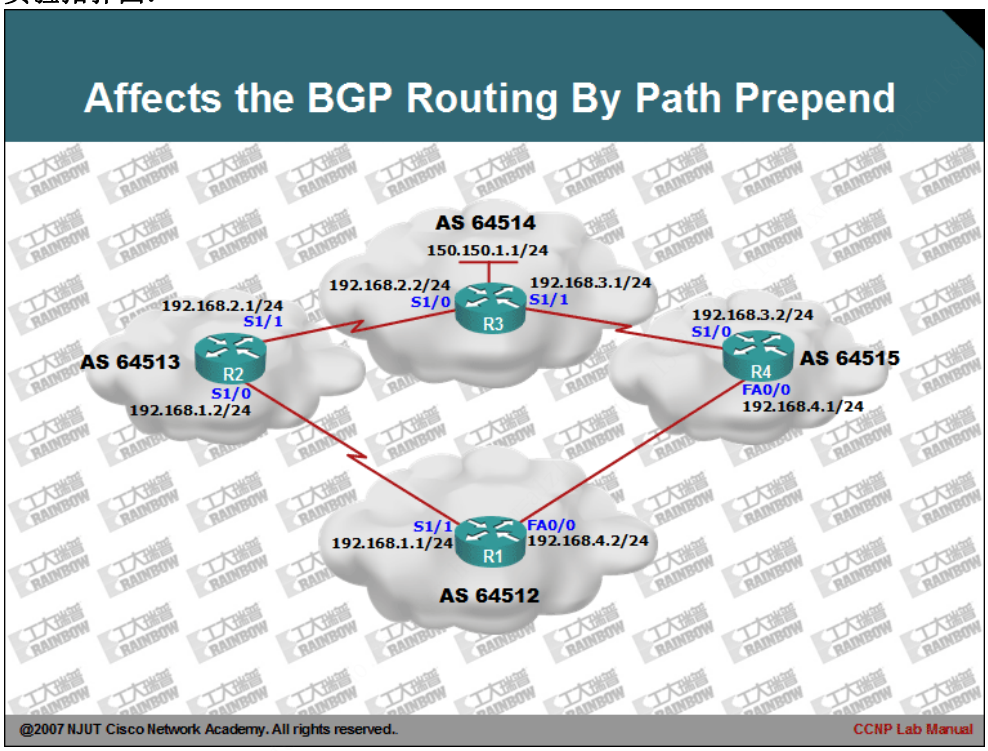
Lab 38. Affects the BGP Routing By Path Prepend

实验目的：

1、掌握如何配置路径欺骗影响 BGP 的路由选择。

2、理解 BGP 的路径欺骗是 MED 的替代解决方法，但是其适用范围较小，只能在有限的网络环境下配置使用。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置各台路由器的 BGP 的协议。

3、查看 R1 的 BGP 的数据库：

```
R1#show ip bgp
BGP table version is 6, local router ID is 192.168.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  150.150.1.0/24   192.168.4.1                           0 64515 64514 i
*>                  192.168.1.2                           0 64513 64514 i
*  192.168.1.0      192.168.4.1                           0 64515 64514 64513 i
*                   192.168.1.2              0            0 64513 i
*>                  0.0.0.0                  0        32768 i
*  192.168.2.0      192.168.4.1                           0 64515 64514 i
*>                  192.168.1.2              0            0 64513 i
*> 192.168.3.0      192.168.4.1              0            0 64515 i
*                   192.168.1.2                           0 64513 64514 i
*  192.168.4.0      192.168.4.1              0            0 64515 i
*                   192.168.1.2                           0 64513 64514 64515 i
*>                  0.0.0.0                  0        32768 i
R1#
```

批注 [stanley372]： 由于 R2 与 R4 同时向 R1 通告 BGP 的路由，**而且其 AS-PATH 路径长度相同。**因此 R1 可能是因此时间差或是 BGP Router-ID 的原因导致了选择 192.168.1.2 作为其下一跳。到达目标网络 150.150.1.0/25。

4、查看 R1 的路由表：

```
R1#show ip route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial1/1
B    192.168.2.0/24 [20/0] via 192.168.1.2, 00:01:20
B    192.168.3.0/24 [20/0] via 192.168.4.1, 00:01:20
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.1.2, 00:01:20
R1#
```

5、在之前实验中，可以通过 MED 和 Local Preference 属性才影响 R1 选择路由。其实还可以通过 AS-PATH 来影响路由选择。其参照的是 **BGP 的选路规则：优先选**

择 AS-PATH 最短的路径。

6、为了验证 AS-PATH 对路由选择的影响，在 R3 路由器上作如下配置：

```
R3(config)#access-list 1 permit 150.150.1.0 0.0.0.255
R3(config)#
R3(config)#route-map set_prepend permit 10
R3(config-route-map)#match ip address 1
R3(config-route-map)#set as-path prepend 64514 64514
R3(config-route-map)#exit
R3(config)#
R3(config)#route-map set_prepend permit 20
R3(config-route-map)#exit
R3(config)#
R3(config)#router bgp 64514
R3(config-router)#neighbor 192.168.2.1 route-map set_prepend out
R3(config-router)#exit
R3(config)#exit
R3#
R3#clear ip bgp * soft out
R3#
```

批注 [stanley373]：匹配 ACL 1 的路由，在其路由的 AS-PATH 尾部添加两个 64514 的自治系统编号。

批注 [stanley374]：对于发向 R2 的路由路由进行策略配置。

需要注意的是：在 set as-path prepend 后添加的 AS 号，最好是本地自治系统号，否则可能会产生无效路由。

7、查看 R1 的 BGP 的数据库：

```
R1#show ip bgp

   Network          Next Hop            Metric LocPrf Weight Path
*> 150.150.1.0/24   192.168.4.1                            0 64515 64514 i
*                   192.168.1.2                            0 64513 64514 64514 64514 i
*  192.168.1.0      192.168.1.2              0             0 64513 i
*>                  0.0.0.0                  0         32768 i
*  192.168.2.0      192.168.4.1                            0 64515 64514 i
*>                  192.168.1.2              0             0 64513 i
*> 192.168.3.0      192.168.4.1              0             0 64515 i
*                   192.168.1.2                            0 64513 64514 i
*  192.168.4.0      192.168.4.1              0             0 64515 i
*>                  0.0.0.0                  0         32768 i
R1#
```

批注 [stanley375]：由于两条路由，拥有不同长度的 AS-PATH。因此 BGP 会选择最短路径的路由到达目标网络。

8、继续查看 R1 的路由表：

```
R1#show ip route

C    192.168.4.0/24 is directly connected, FastEthernet0/0
```

```
C    192.168.1.0/24 is directly connected, Serial1/1
B    192.168.2.0/24 [20/0] via 192.168.1.2, 00:12:54
B    192.168.3.0/24 [20/0] via 192.168.4.1, 00:12:54
     150.150.0.0/24 is subnetted, 1 subnets
B       150.150.1.0 [20/0] via 192.168.4.1, 00:09:42
R1#
```

9、实验完成。

CCNP Lab Manual

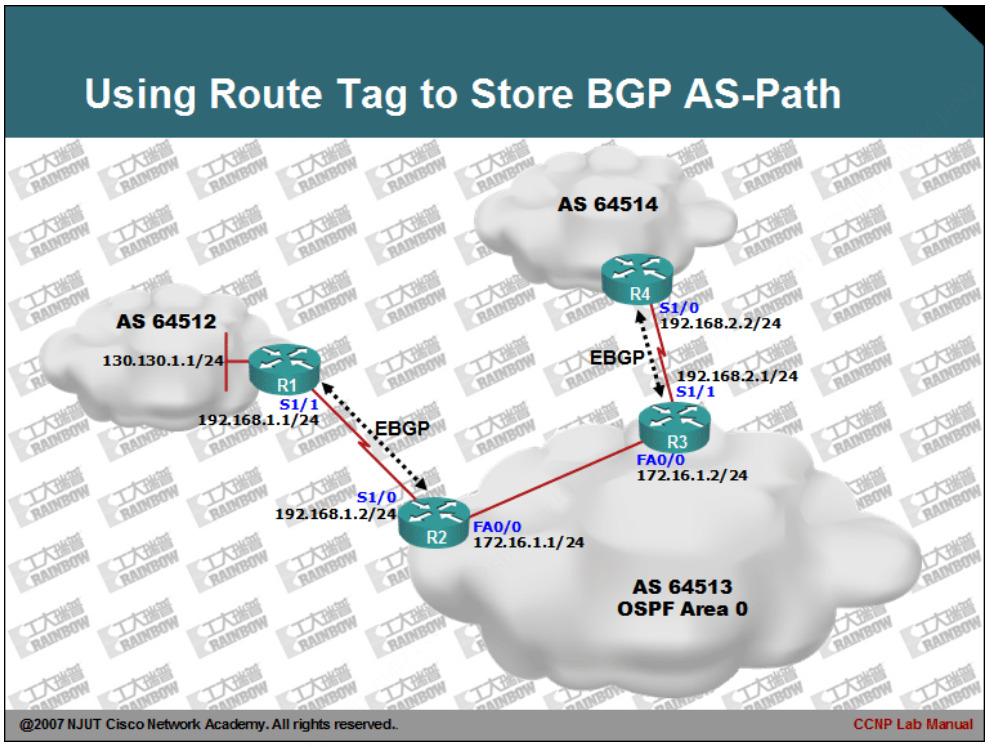
Lab 39. Using Route Tag to Store BGP AS-Path

实验目的：

1、解决 BGP 与 IGP 在做路由重发布时,BGP AS-PATH 属性丢失的问题。

2、掌握使用路由标记存储 BGP 路径属性配置方法。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置 R2 与 R3 的 OSPF 的路由协议，配置如下：

```
R2(config)#router ospf 1
R2(config-router)#network 172.16.1.0 0.0.0.255 area 0
R2(config-router)#exit
R2(config)#exit
```

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.0 0.0.0.255 area 0
R3(config-router)#exit
R3(config)#exit
```

3、确认 R2 与 R3 的 OSPF 的邻居关系。

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.2.1       1   FULL/BDR        00:00:32    172.16.1.2      FastEthernet0/0
R2#
```

4、配置 R1 与 R2，R3 与 R4 之间的 BGP 协议。**注意：R2 与 R4 之间没有任何 BGP 的邻接关系。**

其中 R2 与 R3 的配置如下：

```
R2(config)#router bgp 64513
R2(config-router)#neighbor 192.168.1.1 remote-as 64512
R2(config-router)#network 192.168.1.0 mask 255.255.255.0
R2(config-router)#exit
R2(config)#exit
R2#
```

批注 [stanley376]: R2 仅指定 R1 为 BGP 的邻居。

```
R3(config)#router bgp 64513
R3(config-router)#neighbor 192.168.2.2 remote-as 64514
R3(config-router)#network 192.168.2.0 mask 255.255.255.0
R3(config-router)#exit
R3(config)#exit
```

批注 [stanley377]: R3 仅指定 R4 为邻居。

5、确认 R2 与 R3 的 BGP 的邻接关系。

```
R2#show ip bgp summary
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.1.1     4 64512       8       8        3    0    0 00:03:37        2
```

```
R2#
```

```
R3#show ip bgp summary

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.2     4 64514       6       6        2    0    0 00:01:46        1
R3#
```

6、查看 R4 的路由表。由于 R2 与 R3 之间没有 BGP 的邻接关系。所以 R2 从 R1 学习到的 BGP 路由 150.150.1.0/24 的网络无法转发给 R3 路由器，因此 R4 上本没有学习到任何的路由。

```
R4#show ip route

Gateway of last resort is not set

C    192.168.2.0/24 is directly connected, Serial1/0
R4#
```

7、配置 R2 与 R3 的 BGP 与 OSPF 的重发布，配置如下：

```
R2(config)#router ospf 1
R2(config-router)#redistribute bgp 64513 subnets
R2(config-router)#exit
R2(config)#
R2(config)#router bgp 64513
R2(config-router)#redistribute ospf 1 match external internal
R2(config-router)#
```

批注 [stanley378]：将 OSPF 中的内部与外部类型的路由重发布到 BGP 64513 的自治系统。

```
R3(config)#router bgp 64513
R3(config-router)#redistribute ospf 1 match internal external
R3(config-router)#exit
R3(config)#
R3(config)#router ospf 1
R3(config-router)#redistribute bgp 64513 subnets
R3(config-router)#exit
R3(config)#exit
```

8、查看 R4 的路由表，确认路由的重发布。

```
R4#show ip route

.....

Gateway of last resort is not set
```

```
     172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 192.168.2.1, 00:03:18
     130.130.0.0/24 is subnetted, 1 subnets
B       130.130.1.0 [20/1] via 192.168.2.1, 00:03:18
B    192.168.1.0/24 [20/1] via 192.168.2.1, 00:03:18
C    192.168.2.0/24 is directly connected, Serial1/0
R4#
```

9、查看 R4 的 BGP 的数据库。

```
R4#show ip bgp
BGP table version is 5, local router ID is 192.168.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 130.130.1.0/24   192.168.2.1              1             0 64513 ?
*> 172.16.1.0/24    192.168.2.1              0             0 64513 ?
*> 192.168.1.0      192.168.2.1              1             0 64513 ?
*  192.168.2.0      192.168.2.1              0             0 64513 i
*>                  0.0.0.0                  0         32768 i
R4#
```

批注 [stanley379]: AS-PATH 信息不完整。

10、**产生此 AS-PATH 路径信息丢失的主要原因是：**由于 R2 路由器把 BGP 路由协议重发布到 OSPF 中，而 OSPF 不能够识别 BGP 的路由 AS-PATH 属性。所以在 R4 上查看重发布路由的 AS-PATH 是不完整。

解决这个问题的关键：由于路由标记可以被所有的路由协议识别，因此，可以在重发布前将 BGP 的 AS-PATH 转存到路由标记中，然后在 R4 路由器上再发路由标识中存储的 AS-PATH 取出来还原到 BGP 的路由中。

11、在 R2 上实施路由标记的配置：

```
R2(config)#route-map SET_TAG permit 10
R2(config-route-map)#set automatic-tag
R2(config-route-map)#exit
R2(config)#
R2(config)#router bgp 64513
R2(config-router)#table-map SET_TAG
R2(config-router)#exit
```

批注 [stanley380]: 设置自动计算路由标记。主要计算结果为 AS-PATH 的属性值。

批注 [stanley381]: 配置将 BGP 的扩展属性，映射到路由表中。其主要目的是通过 SET_TAG 的路由图的过滤，将 AS-PATH 将属性存储到标记中。

12、配置 R3 路由器的路由标记。

```
R3(config)#route-map GET_TAG permit 10
```

```
R3(config-route-map)#set as-path tag
R3(config-route-map)#exit
R3(config)#router bgp 64513
R3(config-router)#redistribute ospf 1  match external internal route-map GET_TAG
R3(config-router)#exit
```

批注 [stanley382]：将 AS-PATH 属性从路由标记中取出，并还原到 BGP 的路由数据库中。

批注 [stanley383]：在路由重发布时，完成 AS-PATH 的转存工作。

13、查看 R4 路由器的 BGP 的数据库。

```
R4#show ip bgp
BGP table version is 6, local router ID is 192.168.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 130.130.1.0/24   192.168.2.1              1             0 64513 64512 ?
*> 172.16.1.0/24    192.168.2.1              0             0 64513 ?
*> 192.168.1.0      192.168.2.1              1             0 64513 ?
*  192.168.2.0      192.168.2.1              0             0 64513 i
*>                  0.0.0.0                  0         32768 i
R4#
```

批注 [stanley384]：此时，已经可以在 R4 上能查看到 AS-PATH 的属性信息了。

14、在 R3 上继续配置，以解决路由起源信息不完整的问题。

```
R3(config)#route-map SET_ORIGIN permit 10
R3(config-route-map)#set origin igp
R3(config-route-map)#exit
R3(config)#
R3(config)#router bgp 64513
R3(config-router)#neighbor 192.168.2.2 route-map SET_ORIGIN out
R3(config-router)#exit
R3(config)#
```

批注 [stanley385]：设置相应的起源属性为 IGP。

批注 [stanley386]：调用相应的 route-map 设置起源属性。

15、再次在 R4 路由器上查看 BGP 的数据库。

```
R4#show ip bgp

BGP table version is 15, local router ID is 192.168.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 130.130.1.0/24   192.168.2.1              1             0 64513 64512 i
*> 172.16.1.0/24    192.168.2.1              0             0 64513 i
*> 192.168.1.0      192.168.2.1              1             0 64513 i
*  192.168.2.0      192.168.2.1              0             0 64513 i
*>                  0.0.0.0                  0         32768 i
```

批注 [stanley387]：此时，在 R4 的路由器的 BGP 的数据库，显示的 BGP 学习的路由，其 AS-PATH 和起源属性均已完整。

```
R4#
```

16、使用 PING 命令测试路由的有效性。

```
R4#ping 130.130.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 130.130.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/138/220 ms
R4#
```

17、实验完成。

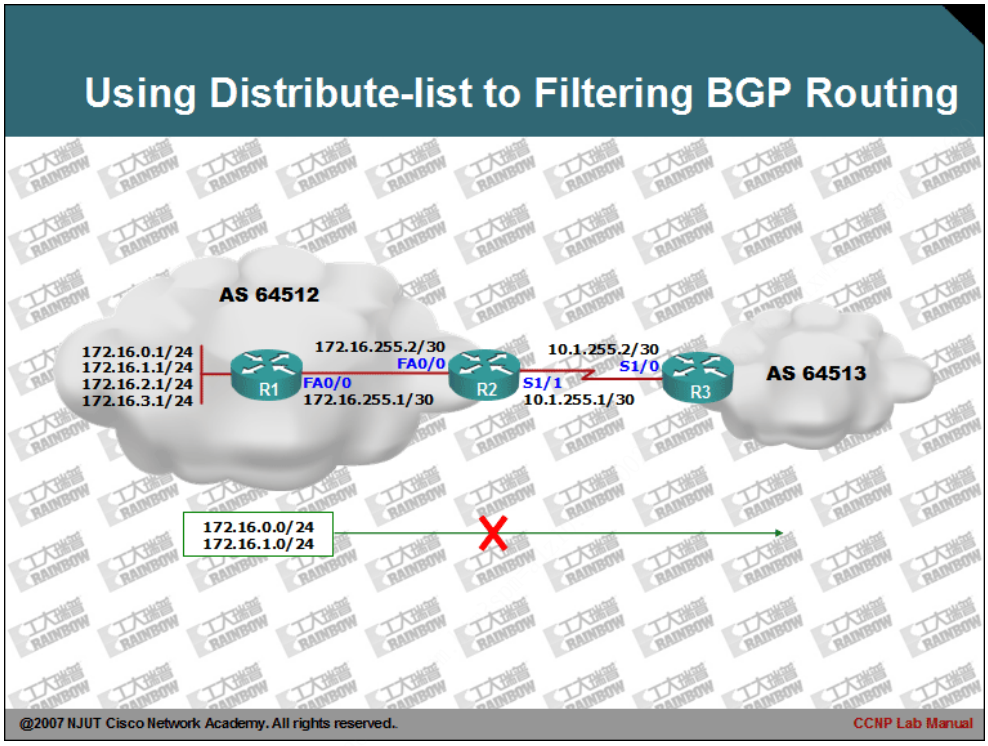
CCNP Lab Manual

Lab 40. Using Distribute-list to Filtering BGP Routing

实验目的：

1、掌握使用 distribute-list 过滤 BGP 的路由。

实验拓扑图：



实验步骤及要求：

1、由于使用 Distribute-list 路由过滤，在**实验：Filtering Routing Updates with a Distribute List** 已经有详细的解释。因此在本次实验中仅列出如何在 BGP 中使用 Distribute-list 命令来进行 BGP 的路由过滤。

2、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

3、配置各台路由器的 BGP 协议，并且关闭 BGP 的自动总结。

4、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:01:43
B       172.16.0.0/24 [20/0] via 10.1.255.1, 00:01:43
B       172.16.1.0/24 [20/0] via 10.1.255.1, 00:01:43
B       172.16.2.0/24 [20/0] via 10.1.255.1, 00:01:43
B       172.16.3.0/24 [20/0] via 10.1.255.1, 00:01:43
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

5、在 R2 配置路由过滤：

```
R2(config)#access-list 1 deny 172.16.0.0 0.0.0.255
R2(config)#access-list 1 deny 172.16.1.0 0.0.0.255
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 10.1.255.2 distribute-list 1 out
R2(config-router)#end
R2#clear ip bgp * soft out
```

批注 [stanley388]: 使用 ACL 标识出需要过滤的路由。

批注 [stanley389]: 针对 10.1.255.2 的对等体进行过滤。

6、查看 R3 的路由表：

```
R3#show ip route

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:06:14
B       172.16.2.0/24 [20/0] via 10.1.255.1, 00:06:14
B       172.16.3.0/24 [20/0] via 10.1.255.1, 00:06:14
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
```

```
R3#
```

7、此时 R3 的路由中的 172.16.0.0/24 和 172.16.1.0/24 的子网已经被成功的过滤。

8、实验完成。

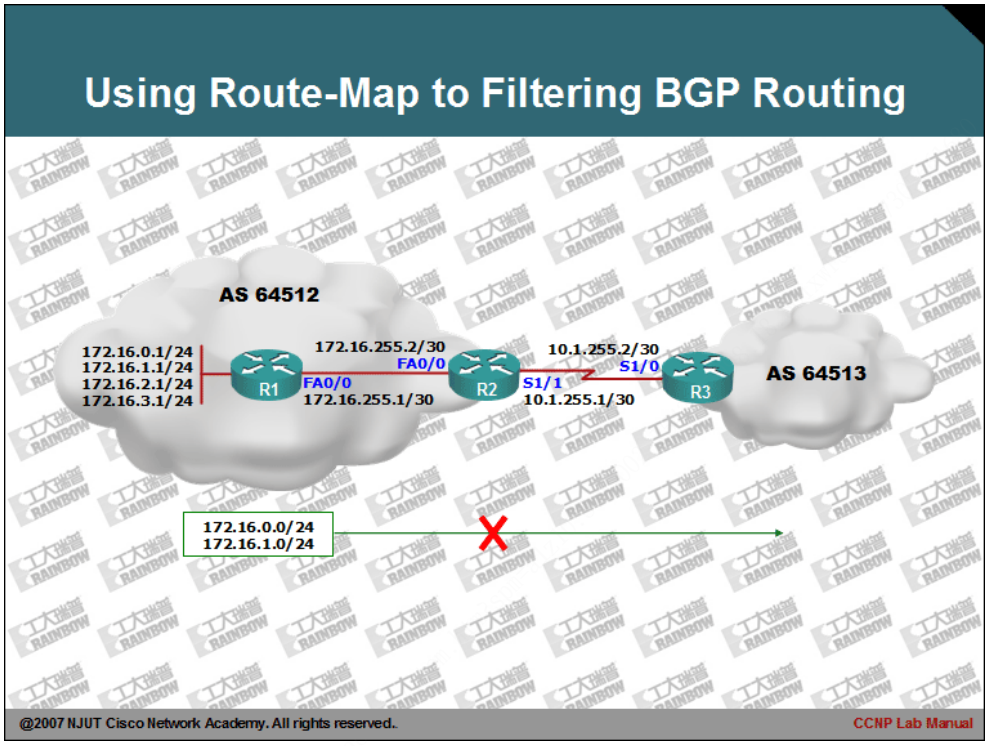
CCNP Lab Manual

Lab 41. Using Route-Map to Filtering BGP Routing

实验目的：

1、掌握使用 Route-Map 过滤 BGP 的路由。

实验拓扑图：



实验步骤及要求：

1、由于使用 Route-Map 路由过滤，在实验：Filtering Routing Updates with a Router Maps

已经有详细的解释。因此在本次实验中仅列出如何在 BGP 中使用 route-map 命令来进行 BGP 的路由过滤。

2、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

3、配置各台路由器的 BGP 的路由协议，，并且关闭 BGP 的自动总结。

4、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:12:39
B       172.16.0.0/24 [20/0] via 10.1.255.1, 00:00:01
B       172.16.1.0/24 [20/0] via 10.1.255.1, 00:00:01
B       172.16.2.0/24 [20/0] via 10.1.255.1, 00:12:39
B       172.16.3.0/24 [20/0] via 10.1.255.1, 00:12:39
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

5、在 R2 上配置 Route-map 路由过滤：

```
R2(config)#access-list 1 deny 172.16.0.0 0.0.0.255
R2(config)#access-list 1 deny 172.16.1.0 0.0.0.255
R2(config)#access-list 1 permit any
R2(config)#
R2(config)#route-map bgpfilter permit 10
R2(config-route-map)#match ip address 1
R2(config-route-map)#exit
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 10.1.255.2 route-map bgpfilter out
R2(config-router)#exit
R2(config)#exit
R2#
R2#clear ip bgp * soft out
R2#
```

批注 [stanley390]：使用 ACL 标识需要过滤的路由。

批注 [stanley391]：创建路由图调用 ACL 1 标识的路由，进行策略匹配。

批注 [stanley392]：针对对等体实施路由过滤。

批注 [stanley393]：加快 BGP 的收敛。

6、查看 R3 的路由表，确认路由过滤的配置：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:19:57
B       172.16.2.0/24 [20/0] via 10.1.255.1, 00:19:57
B       172.16.3.0/24 [20/0] via 10.1.255.1, 00:19:57
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

7、实验完成。

CCNP Lab Manual

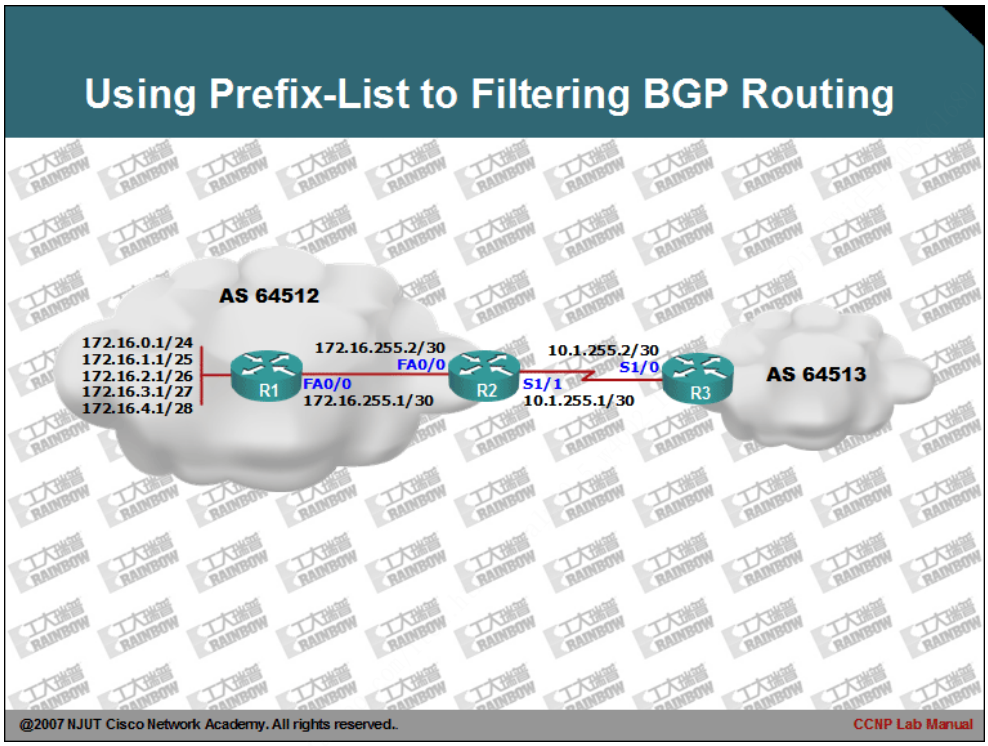
Lab 42. Using Prefix-List to Filtering BGP Routing

实验目的：

1、掌握基于 Prefix-List 的过滤配置方法。

2、掌握 Prefix-List 针对路由的子网掩码长度的选择性过滤配置。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置各台路由器的 BGP 的路由协议，并且关闭 BGP 的自动总结。

3、查看 R3 路由器的路由表，此时 R3 可以学习到来自于 AS 64512 的所有路由条目：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 6 subnets, 6 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:02:56
B       172.16.4.0/28 [20/0] via 10.1.255.1, 00:00:04
B       172.16.0.0/24 [20/0] via 10.1.255.1, 00:01:21
B       172.16.1.0/25 [20/0] via 10.1.255.1, 00:00:04
B       172.16.2.0/26 [20/0] via 10.1.255.1, 00:00:04
B       172.16.3.0/27 [20/0] via 10.1.255.1, 00:00:04
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B       10.1.255.0/30 [20/0] via 10.1.255.1, 00:02:56
C       10.1.255.0/24 is directly connected, Serial1/0
R3#
```

4、**阶段要求 1：R2 允许将 172.16.0.0/24 和 172.16.1.0/25 路由通告给 R3 路由器。**

5、在 R2 上实施路由过滤的配置：

```
R2(config)#ip prefix-list bgpfilter seq 5 deny 172.16.0.0/24
R2(config)#ip prefix-list bgpfilter seq 10 deny 172.16.1.0/25
R2(config)#ip prefix-list bgpfilter seq 15 permit 0.0.0.0/0 le 32
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 10.1.255.2 prefix-list bgpfilter out
R2(config-router)#exit
```

批注 [stanley394]: 使用 prefix-list 匹配需要拒绝的路由。
最后一条 prefix-list 标识了所有路由中仅有小于/32 的子网路由会被匹配。

其类似于标准访问控制列表中的：
access-list 1 permit any

6、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 4 subnets, 4 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:00:16
```

批注 [stanley395]: 对 10.1.255.2 调用前缀列表。

```
B       172.16.4.0/28 [20/0] via 10.1.255.1, 00:00:16
B       172.16.2.0/26 [20/0] via 10.1.255.1, 00:00:16
B       172.16.3.0/27 [20/0] via 10.1.255.1, 00:00:16
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.255.0/24 is directly connected, Serial1/0
R3#
```

批注 [stanley396]: 此时 R3 已经无法学习到被过滤的网络。
即/24 和/25 的网络路由。

7、**阶段要求 2：仅允许将 172.16.3.0/27 子网通告给 R3 路由器。**

8、针对阶段 2 要求，配置如下：

```
R2(config)#ip prefix-list bgpfilter seq 5 permit 172.16.3.0/27
R2(config)#ip prefix-list bgpfilter seq 10 permit 172.16.255.0/30
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 10.1.255.2 prefix-list bgpfilter out
R2(config-router)#exit
R2(config)#
R2#clear ip bgp * soft out
```

9、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:06:15
B       172.16.3.0/27 [20/0] via 10.1.255.1, 00:06:15
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

10、**阶段要求 3：仅允许 172.16.0.0/22 网络下，子网掩码长度大于等于 26 位的子网路由被通告给 R3 路由器。**

11、针对阶段 3 的要求，在 R2 上配置：

```
R2(config)#ip prefix-list bgpfilter seq 5 permit 172.16.0.0/22 ge 26
R2(config)#ip prefix-list bgpfilter seq 5 permit 172.16.255.0/30
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 10.1.255.2 prefix-list bgpfilter out
R2(config-router)#exit
R2(config)#
R2#clear ip bgp * soft out
R2#
```

批注 [stanley397]: ge 表示大于等于的意思

12、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:11:25
B       172.16.2.0/26 [20/0] via 10.1.255.1, 00:01:16
B       172.16.3.0/27 [20/0] via 10.1.255.1, 00:11:25
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

批注 [stanley398]: 172.16.4.0/28 位子网没有出现在 R3 的路由表中主要原因是：其不属于 172.16.0.0/22 网络中的某个子网。

13、阶段要求 3：仅允许 172.16.0.0/22 网络下，子网掩码长度小于等于 25 位的子网路由被通告给 R3 路由器。

```
R2(config)#ip prefix-list bgpfilter seq 5 permit 172.16.0.0/22 le 25
R2(config)#ip prefix-list bgpfilter seq 10 permit 172.16.255.0/30
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#neighbor 10.1.255.2 prefix-list bgpfilter out
R2(config-router)#exit
R2(config)#exit
R2(config)#
R2#clear ip bgp * soft out
R2#
```

批注 [stanley399]: le 指小于等于。

14、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:15:00
B       172.16.0.0/24 [20/0] via 10.1.255.1, 00:01:10
B       172.16.1.0/25 [20/0] via 10.1.255.1, 00:01:10
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

15、阶段要求 4：仅允许 172.16.0.0/22 网络下，子网掩码长度大于等于 25 但同时其小于等于 26 位的子网路由被通告给 R3 路由器。

```
R2(config)#ip prefix-list bgpfilter permit 172.16.0.0/22 ge 25 le 26
R2(config)#ip prefix-list bgpfilter permit 172.16.255.0/30
R2(config)#
R2(config)#router bgp 64512
```

```
R2(config-router)#neighbor 10.1.255.2 prefix-list bgpfilter out
R2(config-router)#end
R2#
R2#clear ip bgp * soft out
```

16、查看 R3 的路由表：

```
R3#show ip route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
B       172.16.255.0/30 [20/0] via 10.1.255.1, 00:19:42
B       172.16.1.0/25 [20/0] via 10.1.255.1, 00:05:53
B       172.16.2.0/26 [20/0] via 10.1.255.1, 00:01:21
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.255.0 is directly connected, Serial1/0
R3#
```

17、实验完成。

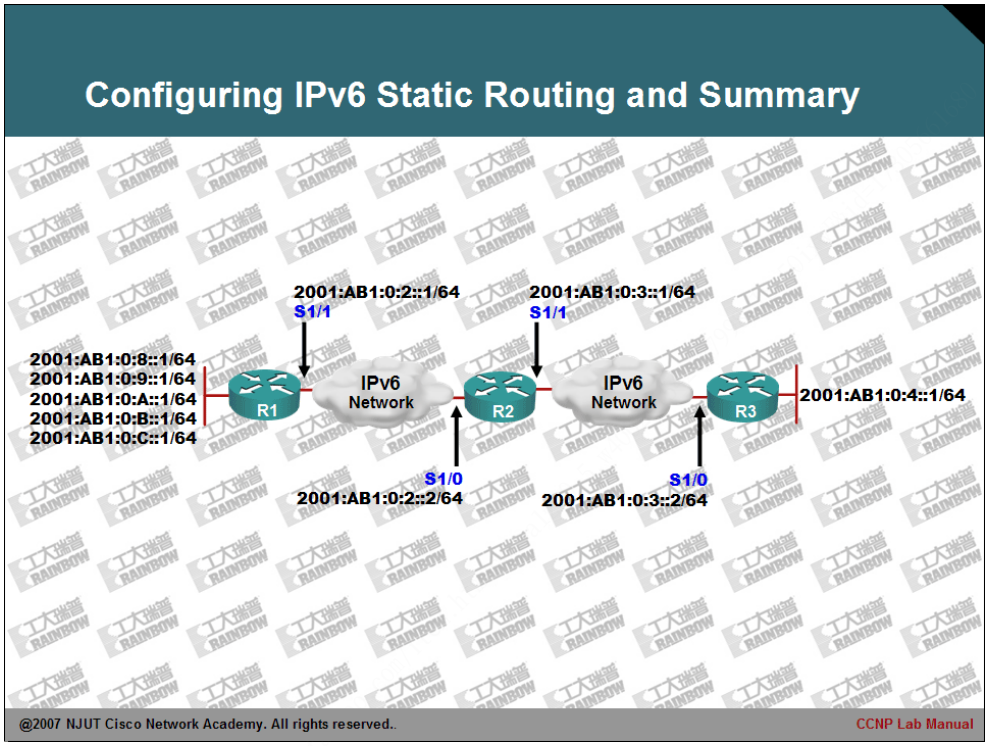
Lab 43. Configuring IPv6 Static Routing and Summary

实验目的：

1、掌握基本的 IPv6 的配置方法。

2、掌握基于 IPv6 的静态路由及路由总结配置。

实验拓扑图：



实验步骤及要求：

1、配置三台路由器的 IPv6 地址，配置如下：

```
R1(config)#
R1(config)#ipv6 unicast-routing
R1(config)#
R1(config)#interface loopback 0
R1(config-if)#ipv6 address 2001:ab1:0:8::1/64
R1(config-if)#ipv6 address 2001:ab1:0:9::1/64
R1(config-if)#ipv6 address 2001:ab1:0:a::1/64
R1(config-if)#ipv6 address 2001:ab1:0:b::1/64
R1(config-if)#ipv6 address 2001:ab1:0:c::1/64
R1(config-if)#exit
R1(config)#
R1(config)#interface serial 1/1
R1(config-if)#ipv6 address 2001:ab1:0:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#
```

批注 [stanley400]: 启用 IPv6 路由。

批注 [stanley401]: 配置 IPv6 地址。由于在 IPv6 网络中，一个接口可以拥有多个网段，所以此处在配置其它地址，并没有像 IPv4 一样，使用 secondary 关键字。

```
R2(config)#ipv6 unicast-routing
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ipv6 address 2001:ab1:0:2::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#inter s 1/1
R2(config-if)#ipv6 address 2001:ab1:0:3::1/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

```
R3(config)#
R3(config)#ipv6 unicast-routing
R3(config)#
R3(config)#interface loopback 0
R3(config-if)#ipv6 address 2001:ab1:0:4::1/64
R3(config-if)#exit
R3(config)#
R3(config)#inter serial 1/0
R3(config-if)#ipv6 address 2001:ab1:0:3::2/64
```

```
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#exit
R3#
```

2、在 R2 路由器上使用 ping 测试与 R1 与 R3 之间的互通性：

```
R2#ping 2001:ab1:0:2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/32 ms
R2#
R2#ping 2001:ab1:0:3::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:3::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/
```

批注 [stanley402]：测试到 R1 的连接。

批注 [stanley403]：到 R3 的连接。

3、查看 R1 的路由表：

```
R1#show ipv6 route

IPv6 Routing Table - 14 entries

C   2001:AB1:0:2::/64 [0/0]
     via ::, Serial1/1
L   2001:AB1:0:2::1/128 [0/0]
     via ::, Serial1/1
C   2001:AB1:0:8::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:8::1/128 [0/0]
     via ::, Loopback0
C   2001:AB1:0:9::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:9::1/128 [0/0]
     via ::, Loopback0
C   2001:AB1:0:A::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:A::1/128 [0/0]
     via ::, Loopback0
C   2001:AB1:0:B::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:B::1/128 [0/0]
```

批注 [stanley404]：查看 ipv6 路由表。

批注 [stanley405]：C 关键字前缀指出本地连接的网段。

批注 [stanley406]：L 关键字前缀，指出此为本地直接主机地址。

```
     via ::, Loopback0
C    2001:AB1:0:C::/64 [0/0]
     via ::, Loopback0
L    2001:AB1:0:C::1/128 [0/0]
     via ::, Loopback0
L    FE80::/10 [0/0]
     via ::, Null0
L    FF00::/8 [0/0]
     via ::, Null0
R1#
```

批注 [stanley407]：FE80 地址前缀为链路本地单播地址，其主要用于 OSPF 等路由协议更新时作为其更新源地址。

批注 [stanley408]：多播地址。

3、在所有路由器上配置到其它非直连网络的静态路由，配置如下：

```
R1(config)#ipv
R1(config)#ipv6 route 2001:ab1:0:3::/64 2001:ab1:0:2::2
R1(config)#
R1(config)#ipv6 route 2001:ab1:0:4::/64 2001:ab1:0:2::2
R1(config)#
```

批注 [stanley409]：IPv6 的静态路由配置与 IPv4 类似。
具体解释是：到达 2001:ab1:0:3::/64 的网络，其下一跳为 2001:ab1:0:2::2。

```
R2(config)#
R2(config)#ipv6 route 2001:ab1:0:4::/64 2001:ab1:0:3::2
R2(config)#
R2(config)#ipv6 route 2001:ab1:0:8::/62 2001:ab1:0:2::1
R2(config)#
R2(config)#ipv6 route 2001:ab1:0:c::/64 2001:ab1:0:2::1
R2(config)#
```

批注 [stanley410]：到达 R3 的环回口路由。

批注 [stanley411]：到达 R1 环回口的汇总路由。

批注 [stanley412]：到达 R1 环回口的不可汇总网段路由。

IPv6 网络的子网汇总与 v4 网络类似。需要注意的是一个 IPv6 的地址字符为 16 进制，每缩减一个字符，对应二进制为四位。如下表所示，即针对 R1 路由器的环回口汇总方法，简单的说，仍然是找同相同的前缀。

2001:ab1:0:8::1	->	2001:ab1:0:0000 0000 0000 10 00::1	2001：ab1:0:8::/62
2001:ab1:0:9::1	->	2001:ab1:0:0000 0000 0000 10 01::1	
2001:ab1:0:a::1	->	2001:ab1:0:0000 0000 0000 10 10::1	
2001:ab1:0:b::1	->	2001:ab1:0:0000 0000 0000 10 11::1	
2001:ab1:0:c::1	->	2001:ab1:0:0000 0000 0000 11 00::1	2001:ab1:0:c::/62

```
R3(config)#
R3(config)#ipv6 route ::/0 2001:ab1:0:3::1
R3(config)#
```

批注 [stanley413]：本例中 R3 路由器可以将其认为是 stub 网络路由器，可以配置静态默认路由，简化路由的配置。

4、查看 R2 和 R3 路由表，确认静态路由配置：

```
R2#
```

```
R2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:AB1:0:2::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:2::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/1
L   2001:AB1:0:3::1/128 [0/0]
     via ::, Serial1/1
S   2001:AB1:0:4::/64 [1/0]
     via 2001:AB1:0:3::2
S   2001:AB1:0:8::/62 [1/0]
     via 2001:AB1:0:2::1
S   2001:AB1:0:C::/64 [1/0]
     via 2001:AB1:0:2::1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R2#
```

批注 [stanley414]： 手工配置的静态路由，其管理距离为 1。

```
R3#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2001:AB1:0:3::1
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
```

批注 [stanley415]： R3 路由器的静态默认路由。

```
     via ::, Loopback0
L    FE80::/10 [0/0]
     via ::, Null0
L    FF00::/8 [0/0]
     via ::, Null0
R3#
```

5、在 R3 上测试静态路由有效性：

```
R3#
R3#ping 2001:ab1:0:9::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:9::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/149/192 ms
R3#
R3#
R3#ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:ab1:0:c::1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: y
UDP protocol? [no]:
Precedence [0]:
DSCP [0]:
Include extension headers? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:C::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/145/192 ms
R3#
```

批注 [stanley416]: 此外演示了扩展的 IPv6 的 ping 命令。

6、在 R1 上测试静态路由有效性：

```
R1#ping 2001:ab1:0:4::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:4::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/67/108 ms
R1#
```

7、实验完成。

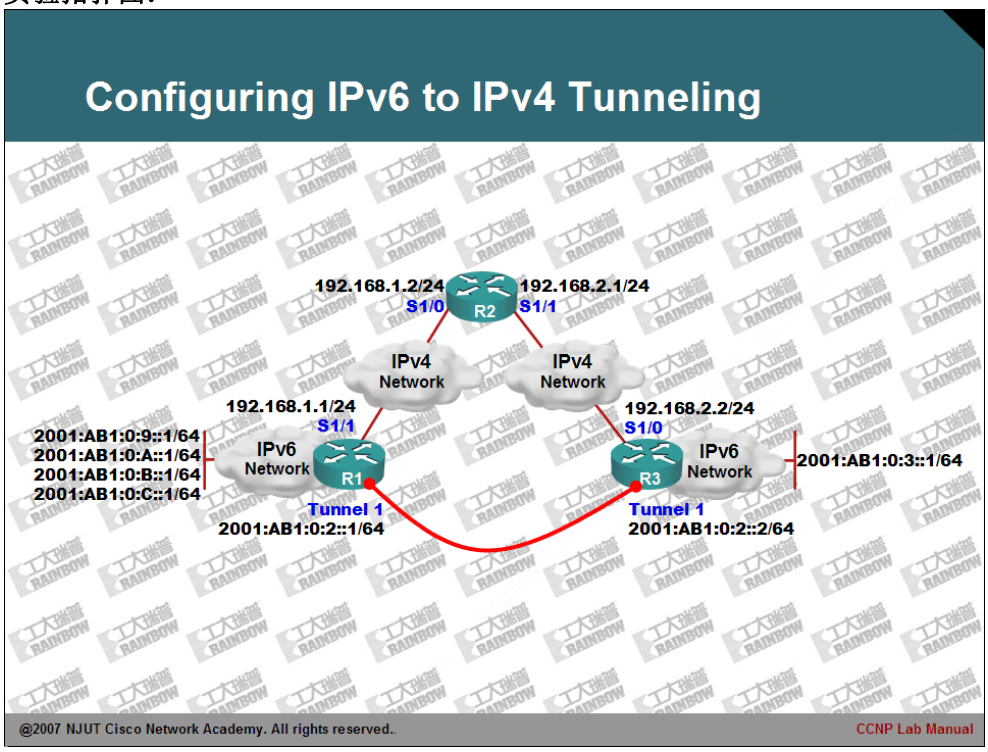
CCNP Lab Manual

Lab 44. Configuring IPv6 to IPv4 Tunneling

实验目的：

1、掌握 6to4 的隧道 GRE 配置方法.

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IPv4 及 v6 地址，并使用 ping 命令测试 v4 网络的互通。同时为 IPv4 网络配置 RIP 或 OSPF 路由协议，保证 v4 网络可路由性。具体路由协议请自行决定。

2、在 R1 上使用 ping 测试到 R3 路由器的 serial 1/0 接口：

```
R1#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/66/72 ms
R1#
```

3、配置 R1 与 R3 的 IPv6 网络地址。

4、在 R1 上配置 GRE 隧道，用于解决 IPv6 网络相互访问需求，配置如下：

```
R1(config)#
R1(config)#interface tunnel 1
R1(config-if)#
R1(config-if)#ipv6 address 2001:ab1:0:2::1/64
R1(config-if)#
R1(config-if)#tunnel source 192.168.1.1
R1(config-if)#
R1(config-if)#tunnel destination 192.168.2.2
R1(config-if)#
R1(config-if)#tunnel mode ipv6ip
R1(config-if)#
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

批注 [stanley417]： 启用 GRE 隧道接口 1。

批注 [stanley418]： 为隧道接口配置 IPv6 地址。

批注 [stanley419]： 配置隧道源端口。

批注 [stanley420]： 配置隧道目标。

注意： 到达此目标地址的路由必须存在于本地 IPv4 网络路由表中。

批注 [stanley421]： 配置隧道模式为 ipv6 over ip 模式。此命令为可选配置。

```
R3(config)#
R3(config)#interface tunnel 2
R3(config-if)#ipv6 address 2001:ab1:0:2::2/64
R3(config-if)#tunnel source serial 1/0
R3(config-if)#tunnel destination 192.168.1.1
R3(config-if)#tunnel mode ipv6ip
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

批注 [stanley422]： 此处使用本地端口号描述的隧道源。

5、有关于 GRE 隧道请参关 **ISCW 实验 Configuring GRE Tunnels**。

6、在 R1 或 R3 上使用 ping 命令测试隧道的配置：

```
R1#
R1#ping 2001:ab1:0:2::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:2::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/67/96 ms
R1#
```

7、查看 R3 路由表：

```
R3#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:AB1:0:2::/64 [0/0]
     via ::, Tunnel2
L   2001:AB1:0:2::2/128 [0/0]
     via ::, Tunnel2
C   2001:AB1:0:3::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:3::1/128 [0/0]
     via ::, Loopback0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

批注 [stanley423]：此路由指出可以通过隧道直接到达 R1 路由器。

8、根据 R1 与 R3 的路由表显示，继续配置如下静态路由：

```
R1(config)#
R1(config)#ipv6 route 2001:ab1:0:3::/64 2001:ab1:0:2::2
R1(config)#
```

批注 [stanley424]：到达目标网络其下一跳为隧道对端的 IPv6 地址。

```
R3(config)#
R3(config)#ipv6 route ::/0 2001:ab1:0:2::1
R3(config)#
```

9、在 R1 或 R3 上使用 ping 命令，测试两端的 IPv6 网络是否可以正常访问：

```
R1#ping 2001:ab1:0:3::1

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:3::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/73/104 ms
R1#
```

```
R3#
R3#ping 2001:ab1:0:9::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:9::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/66/84 ms
R3#
R3#
R3#ping 2001:ab1:0:c::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:C::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/60/76 ms
R3#
```

10、实验完成。

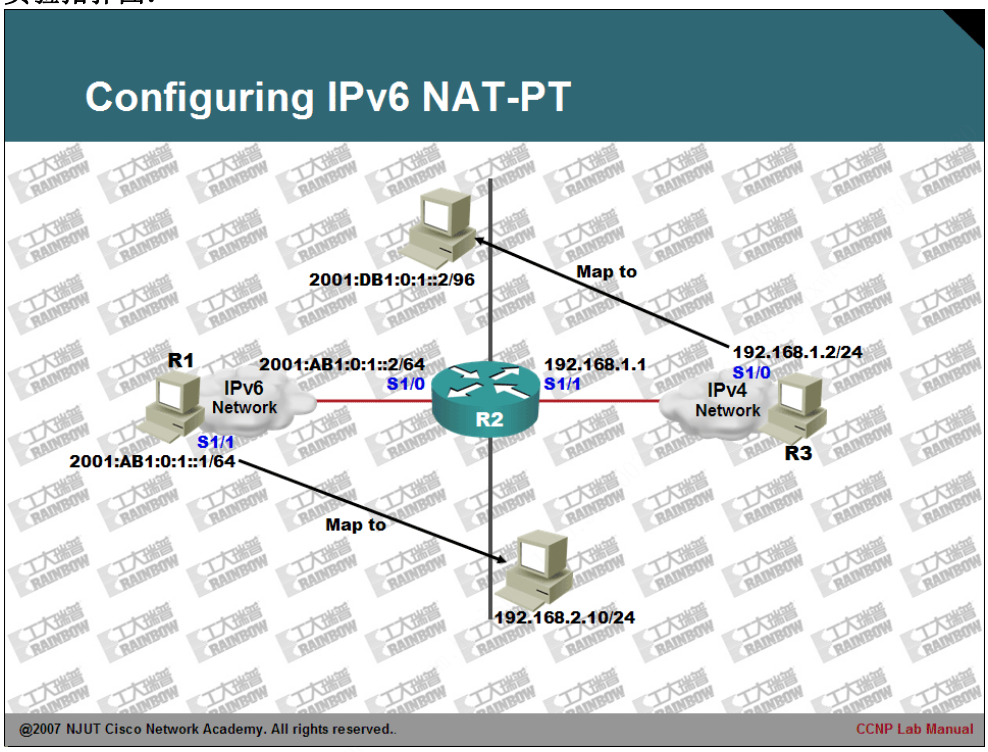
CCNP Lab Manual

Lab 45. Configuring IPv6 NAT-PT

实验目的：

1、掌握 IPv6v4 的静态 NAT-PT 配置。

实验拓扑图：



实验步骤及要求：

1、配置各路由器的 v4 与 v6 地址，并使用 ping 命令测试互通性。

2、在 R1 与 R3 上配置静态路由，其主要目的是描述到达未知网络需要向数据包发送到 NAT-PT 设备进行 v6v4 地址转换。具体配置如下：

```
R1(config)#
R1(config)#ipv6 route ::/0 2001:ab1:0:1::2
R1(config)#
```

```
R3(config)#
R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
R3(config)#
```

3、在 R2 上配置 NAT-PT 进行 v4 到 v6 和 v6 到 v4 的地址转换，具体配置如下：

```
R2(config)#ipv6 unicast-routing
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ipv6 nat
R2(config-if)#exit
R2(config)#
R2(config)#inter serial 1/1
R2(config-if)#ipv6 nat
R2(config-if)#exit
R2(config)#
R2(config)#ipv6 nat v4v6 source 192.168.1.2 2001:db1:0:1::2
R2(config)#
R2(config)#ipv6 nat v6v4 source 2001:ab1:0:1::1 192.168.2.10
R2(config)#
R2(config)#ipv6 nat prefix 2001:db1:0:1::/96
R2(config)#
```

批注 [stanley425]：启用此接口的 IPv6 NAT 功能。

批注 [stanley426]：配置 v4 主机地址到 v6 网络的映射。

批注 [stanley427]：配置 v6 主机地址到 v4 网络的映射。

批注 [stanley428]：根据 RFC 文档规定，被转换后 v6 地址其前缀必须为/96 长度。

4、查看 R2 的地址转换关系表：

```
R2#show ipv6 nat translations
Prot  IPv4 source              IPv6 source
      IPv4 destination         IPv6 destination
---   ---                      ---
      192.168.1.2              2001:DB1:0:1::2

---   192.168.2.10             2001:AB1:0:1::1
      ---                      ---
R2#
```

5、在 R1 和 R3 上使用 ping 命令，测试地址转换：

```
R1#ping 2001:db1:0:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB1:0:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/73/120 ms
R1#
```

```
R3#ping 192.168.2.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/73/92 ms
R3#
```

5、在 R2 上使用 debug 命令查看地址转换的过程：

```
R2#debug ipv6 nat
IPv6 NAT-PT debugging is on
R2#
R2#
R2#
*Sep 12 00:34:28.159: IPv6 NAT: icmp src (192.168.1.2) -> (2001:DB1:0:1::2), dst
(192.168.2.10) -> (2001:AB1:0:1::1)
*Sep 12 00:34:28.175: IPv6 NAT: icmp src (2001:AB1:0:1::1) -> (192.168.2.10), dst
(2001:DB1:0:1::2) -> (192.168.1.2)
R2#
```

6、实验完成。

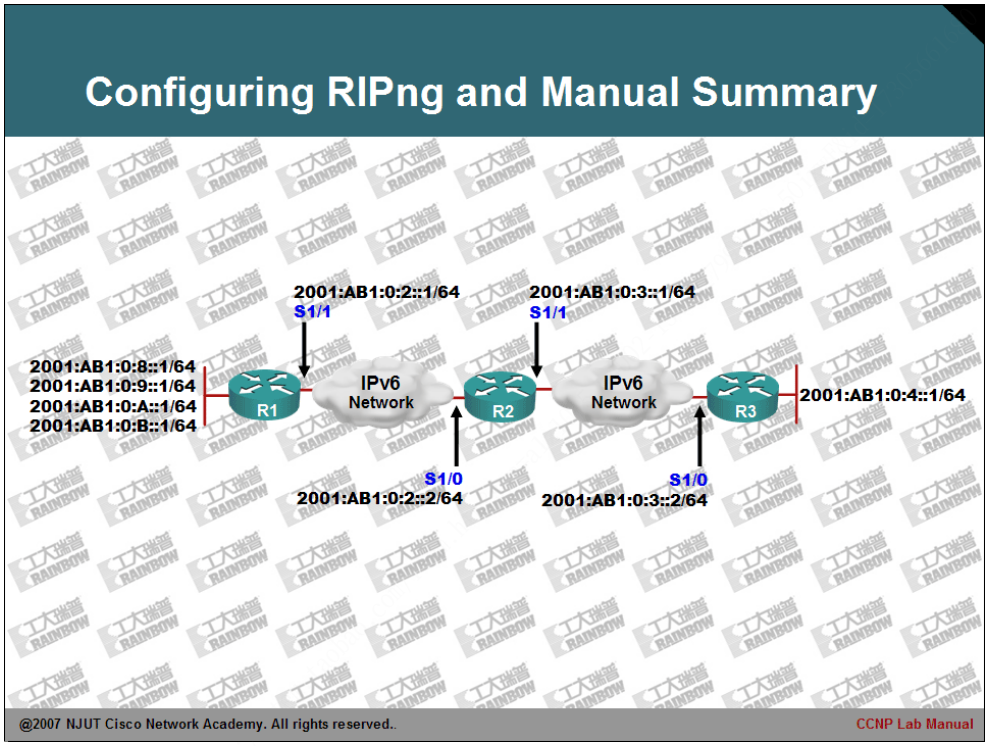
CCNP Lab Manual

Lab 46. Configuring RIPng and Manual Summary

实验目的：

1、掌握基于 IPv6 的 RIPng 配置方法。
2、掌握 RIPng 的手工汇总配置。
3、掌握 RIPng 度量计算及修改方法。
4、掌握调试 RIPng 配置命令。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IPv6 地址，并且使用 ping 命令确认直连接口互通性。

2、在三台路由器上配置 RIPng 路由协议，配置如下所示：

```
R1(config)#
R1(config)#ipv6 router rip wy_rip
R1(config-rtr)#exit
R1(config)#
R1(config)#interface loopback 0
R1(config-if)#ipv6 rip wy_rip enable
R1(config-if)#exit
R1(config)#
R1(config)#interface serial 1/1
R1(config-if)#ipv6 rip wy_rip enable
R1(config-if)#exit
R1(config)#exit
R1#
```

批注 [stanley429]：全局启用 RIPng 协议，wy_rip 类似于进程标识符。

批注 [stanley430]：接口下针对 wy_rip 进程启用 RIPng 路由。

```
R2(config)#ipv6 router rip wy_rip
R2(config-rtr)#exit
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ipv6 rip wy_rip enable
R2(config-if)#exit
R2(config)#
R2(config)#interface serial 1/1
R2(config-if)#ipv6 rip wy_rip enable
R2(config-if)#exit
R2(config)#exit
```

```
3(config)#ipv6 router rip wy_rip
R3(config-rtr)#exit
R3(config)#
R3(config)#interface serial 1/0
R3(config-if)#ipv6 rip wy_rip enable
R3(config-if)#exit
R3(config)#
R3(config)#interface loopback 0
R3(config-if)#ipv6 rip wy_rip enable
R3(config-if)#exit
R3(config)#exit
R3#
```

3、查看 R3 路由器路由表：

```
R3#show ipv6 route
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R   2001:AB1:0:2::/64 [120/2]
     via FE80::C801:EFF:FEAC:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
R   2001:AB1:0:8::/64 [120/3]
     via FE80::C801:EFF:FEAC:0, Serial1/0
R   2001:AB1:0:9::/64 [120/3]
     via FE80::C801:EFF:FEAC:0, Serial1/0
R   2001:AB1:0:A::/64 [120/3]
     via FE80::C801:EFF:FEAC:0, Serial1/0
R   2001:AB1:0:B::/64 [120/3]
     via FE80::C801:EFF:FEAC:0, Serial1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R3#
```

批注 [stanley431]： RIPng 管理距离与 IPv4 的 RIP 协议一致，均为 120 的管理距离。

批注 [stanley432]： 需要注意的是，RIPng 的度量与 RIP 协议不同的是，路由再进入路由表时加 1。而 RIP 路由协议在路由向外通告时加 1。

4、查看 RIPng 的路由协议参数：

```
R3#show ipv6 rip
RIP process "wy_rip", port 521, multicast-group FF02::9, pid 129
     Administrative distance is 120. Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 9, trigger updates 3
  Interfaces:
    Loopback0
```

批注 [stanley433]： 此处分别显示了，进程标识符，UDP 端口号和组播地址。

```
    Serial1/0
  Redistribution:
    None
```

5、观察负载均衡路径数量：

```
R3(config)#ipv6 router rip wy_rip
R3(config-rtr)#maximum-paths ?
  <1-64>  Number of paths
```

批注 [stanley434]：RIPng 默认开启了 16 条路径的负载均衡，其最大支持 64 条路径负载均衡。

6、在 R3 上使用 debug 命令观察 RIPng 的通告：

```
R3#debug ipv6 rip
RIP Routing Protocol debugging is on
R3#
*Sep 12 01:46:59.275: RIPng: Sending multicast update on Loopback0 for wy_rip
*Sep 12 01:46:59.275:        src=FE80::C802:EFF:FEAC:0
*Sep 12 01:46:59.279:        dst=FF02::9 (Loopback0)
*Sep 12 01:46:59.279:        sport=521, dport=521, length=152
*Sep 12 01:46:59.279:        command=2, version=1, mbz=0, #rte=7
*Sep 12 01:46:59.283:        tag=0, metric=2, prefix=2001:AB1:0:2::/64
*Sep 12 01:46:59.283:        tag=0, metric=1, prefix=2001:AB1:0:3::/64
*Sep 12 01:46:59.283:        tag=0, metric=1, prefix=2001:AB1:0:4::/64
*Sep 12 01:46:59.287:        tag=0, metric=3, prefix=2001:AB1:0:8::/64
*Sep 12 01:46:59.287:        tag=0, metric=3, prefix=2001:AB1:0:9::/64
*Sep 12 01:46:59.287:        tag=0, metric=3, prefix=2001:AB1:0:A::/64
*Sep 12 01:46:59.291:        tag=0, metric=3, prefix=2001:AB1:0:B::/64
*Sep 12 01:46:59.295: RIPng: Sending multicast update on Serial1/0 for wy_rip
*Sep 12 01:46:59.295:        src=FE80::C802:EFF:FEAC:0
*Sep 12 01:46:59.295:        dst=FF02::9 (Serial1/0)
*Sep 12 01:46:59.295:        sport=521, dport=521, length=52
*Sep 12 01:46:59.299:        command=2, version=1, mbz=0, #rte=2
*Sep 12 01:46:59.299:        tag=0, metric=1, prefix=2001:AB1:0:3::/64
*Sep 12 01:46:59.299:        tag=0, metric=1, prefix=2001:AB1:0:4::/64
*Sep 12 01:46:59.303: RIPng: Process wy_rip received own response on Loopback0
R3#
```

批注 [stanley435]：RIPng 默认使用 FE80 的链路本地地址进行路由通告。

批注 [stanley436]：通告的目标为组播地址 FF02，其范围与 v4 的 224.0.0.2 一致。

批注 [stanley437]：本地路由表中路由在通告给其它路由器时，并不会为其度量加 1。

7、使用 ping 命令确认路由有效性：

```
R3#ping 2001:ab1:0:8::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:8::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/113/188 ms
R3#
```

8、通过第三步显示的路由器可以看出，RIPng 并不能够自动路由总结，因此在 R1 上实施路由手工汇总进行路由优化，配置如下：

```
R1(config)#
R1(config)#interface serial 1/1
R1(config-if)#ipv6 rip wy_rip summary-address 2001:ab1:0:8::/62
R1(config-if)#
```

批注 [stanley438]：此命令用于汇总 RIPng 发出的路由。

9、再次观察 R3 路由表，确认汇总：

```
R3#
R3#clear ipv6 rip wy_rip
R3#clear ipv6 route *
R3#
R3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R   2001:AB1:0:2::/64 [120/2]
     via FE80::C801:EFF:FEAC:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
R   2001:AB1:0:8::/62 [120/3]
     via FE80::C801:EFF:FEAC:0, Serial1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R3#
```

批注 [stanley439]：使用 clear 命令刷新 RIPng 和路由表，加快收敛。
必要时，需要在所有路由器上使用本命令，加快收敛。

批注 [stanley440]：被 R1 汇总后的 RIPng 路由。
其度量值，即跳数为 3。

10、RIPng 还提供了手工修改度量值，即在路由进入路由表时，确定对度量值如何处理，演示示例如下：

```
R3(config)#interface serial 1/0
R3(config-if)#ipv6 rip wy_rip metric-offset 10
R3(config-if)#
```

批注 [stanley441]：针对此接口学习到的路由，对其度量跳数进行加 10 处理。

默认行为是加 1。

11、查看 R3 路由表，确认度量值变动：

```
R3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R   2001:AB1:0:2::/64 [120/11]
     via FE80::C801:EFF:FEAC:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
R   2001:AB1:0:8::/62 [120/12]
     via FE80::C801:EFF:FEAC:0, Serial1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R3#
```

批注 [stanley442]: 度量值由默认的 3 被修改为 12。

12、实验完成。

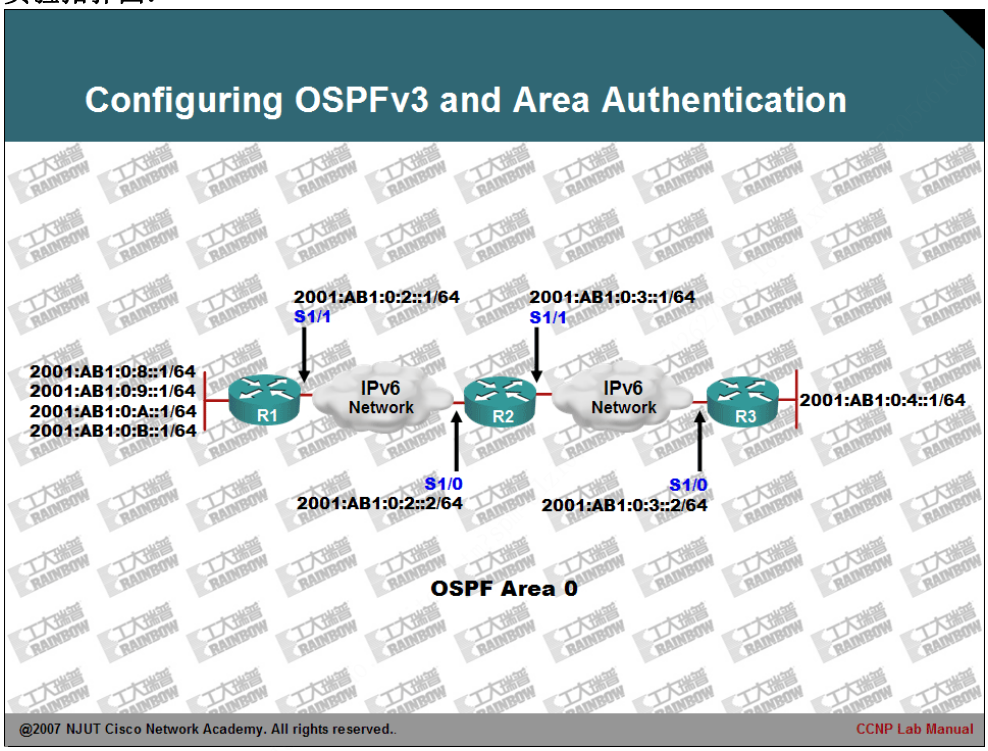
CCNP Lab Manual

Lab 47. Configuring OSPFv3 and Area Authentication

实验目的：

1、掌握基于 IPv6 的 OSPF 配置方法。
2、掌握基于 IPsec 的 OSPF 的认证配置。
3、监视 OSPFv3 工作。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IPv6 地址，并且使用 ping 命令确认直连接口的互通性。

2、在 R1，R2 和 R3 路由器上配置 OSPFv3 路由协议，配置如下：

```
R1(config)#ipv6 router ospf 20
R1(config-rtr)#
*Sep 12 02:22:14.499: %OSPFv3-4-NORTRID: OSPFv3 process 20 could not pick a router-id,
please configure manually
R1(config-rtr)#
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#
R1(config)#interface serial 1/1
R1(config-if)#ipv6 ospf 20 area 0
R1(config-if)#exit
R1(config)#
R1(config)#interface loopback 0
R1(config-if)#ipv6 ospf 20 area 0
R1(config-if)#ipv6 ospf network point-to-point
R1(config-if)#exit
R1(config)#
```

批注 [stanley443]： 全局启用 OSPF 路由，进程号为 20。

批注 [stanley444]： 由于 OSPFv3 虽然用于 IPv6 网络路由，但是其 router-id 仍然为 32bit,OSPFv3 在启用时，会自动的寻找本地是否配置 IPv4 地址以便使用其作为 router-id,如果本地没有配置，因此需要手工配置一个 router-id。

批注 [stanley445]： 将接口加入到 OSPF 的进程中。并且指定其属于 area 0 的区域。

批注 [stanley446]： 配置环回口网络类型为 P2P,以避免向外通告/128 的主机路由。

```
R2(config)#
R2(config)#ipv6 router ospf 30
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#exit
R2(config)#
R2(config)#interface serial 1/1
R2(config-if)#ipv6 ospf 30 area 0
R2(config-if)#exit
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ipv6 ospf 30 area 0
R2(config-if)#exit
R2(config)#
```

```
R3(config)#
R3(config)#ipv6 router ospf 40
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#exit
R3(config)#
R3(config)#
```

```
R3(config)#interface loopback 0
R3(config-if)#ipv6 ospf 40 area 0
R3(config-if)#ipv6 ospf network point-to-point
R3(config-if)#exit
R3(config)#
R3(config)#interface serial 1/0
R3(config-if)#ipv6 ospf 40 area 0
R3(config-if)#exit
R3(config)#exit
*Sep 12 02:29:42.415: %OSPFv3-5-ADJCHG: Process 40, Nbr 2.2.2.2 on Serial1/0 from LOADING to
FULL, Loading Done
R3#
```

批注 [stanley447]：系统提示 OSPF 的邻居关系已经成功创建。

3、在 R2 上查看 OSPF 的邻居关系：

```
R2#show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
1.1.1.1           1   FULL/  -        00:00:32    4               Serial1/0
3.3.3.3           1   FULL/  -        00:00:30    3               Serial1/1

R2#
```

批注 [stanley448]：由于连接采用 serial 接口，其接口默认类型为 P2P，因此无需要选举 DR 和 BDR。

4、在 R3 上查看 OSPF 的数据库：

```
R3#show ipv6 ospf database

            OSPFv3 Router with ID (3.3.3.3) (Process ID 40)

                Router Link States (Area 0)
ADV Router      Age         Seq#       Fragment ID  Link count  Bits
1.1.1.1         645         0x80000003 0            1           None
2.2.2.2         543         0x80000003 0            2           None
3.3.3.3         543         0x80000002 0            1           None

                Link (Type-8) Link States (Area 0)
ADV Router      Age         Seq#       Link ID     Interface
2.2.2.2         658         0x80000001 4           Se1/0
3.3.3.3         543         0x80000001 3           Se1/0

                Intra Area Prefix Link States (Area 0)
ADV Router      Age         Seq#       Link ID     Ref-lstype  Ref-LSID
1.1.1.1         878         0x80000002 0           0x2001      0
2.2.2.2         646         0x80000002 0           0x2001      0
3.3.3.3         543         0x80000002 0           0x2001      0
```

批注 [stanley449]：LSA 0X2001 此类型 LSA 仅仅用于描述区域内链路上的邻居信息。
其会在区域内泛洪。

批注 [stanley450]：LSA 0X2008 此类型 LSA 仅仅用于描述直连路由器邻居间链路上的 IPv6 的前缀信息。其泛洪范围限制在本地链路上。

批注 [stanley451]：LSA 0X2009 此类型 LSA 用于提供拓扑信息，类似于 v4 的 OSPFv2 的 LSA 1。用于通告已知的 IPv6 前缀信息。
其泛洪范围为区域内。

5、查看 R3 路由表：

```
R3#show ipv6 route
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001:AB1:0:2::/64 [110/128]
     via FE80::C801:EFF:FEAC:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
O   2001:AB1:0:8::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
O   2001:AB1:0:9::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
O   2001:AB1:0:A::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
O   2001:AB1:0:B::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R3#
```

批注 [stanley452]: OSPFv3 管理距离为 110。

6、使用 ping 命令确认路由有效性：

```
R3#ping 2001:ab1:0:8::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:8::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/91/120 ms
R3#
```

7、另外可以通过配置区域认证，确保 OSPFv3 的安全性。**由于目前尚没有能够支持 OSPFv3 认证的 IOS 版本，因此仅给出配置命令示例。请各位自行测试，如果可能的话，请您与我(王远，stanley.wy，QQ：7625526)联系，共享 IOS，多谢。**

另外由于无法实中践，因此仅供参考。

```
R1(config)#ipv6 router ospf 20
R1(config-rtr)#area 0 authentication ipsec spi 600 md5 1234567890ABCDEF1234567890ABCDEF
R1(config-rtr)#
```

批注 [stanley453]: 配置基于 IPsec 的 OSPF 的区域认证。
SPI 号为安全关联索引值，MD5 为加密算法，其后追加为密钥值。

8、实验完成。

CCNP Lab Manual

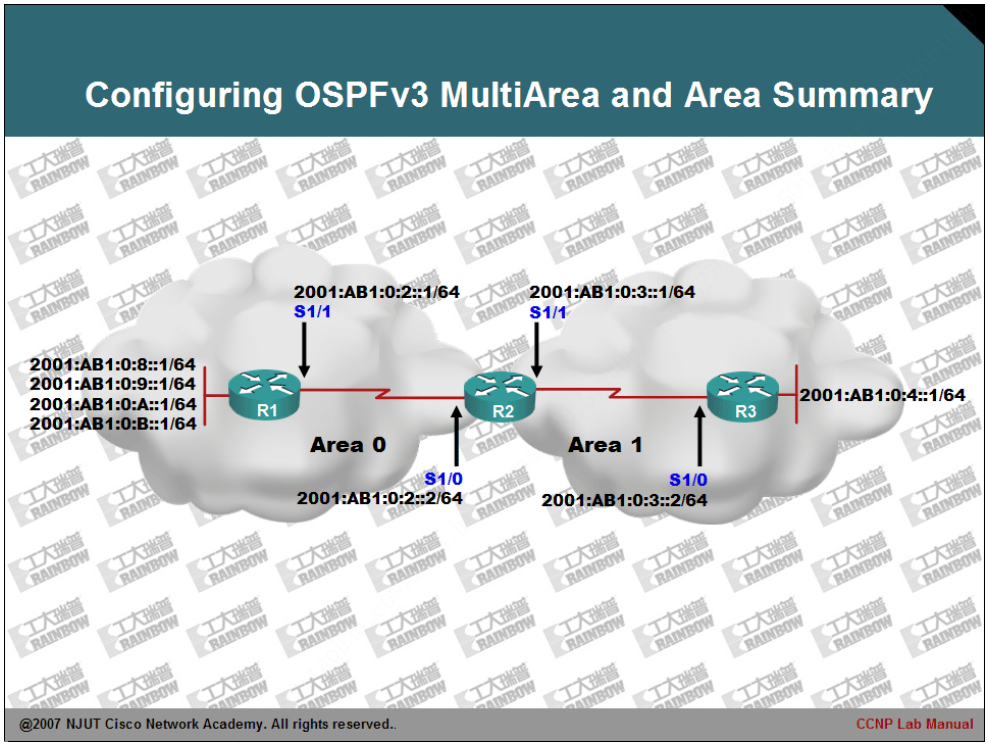
Lab 48. Configuring OSPFv3 MultiArea and Area Summary

实验目的：

1、掌握基于 IPv6 的 OSPF 多区域配置方法。

2、配置 OSPFv3 的区域汇总。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IPv6 地址，并且使用 ping 命令确认直连接口的互通性。

2、由于本实验与 OSPFv2 配置极为类似，因此仅给了 R2 路由器的 OSPFv3 的配置，其它路由器请自行配置。

```
R2(config)#
R2(config)#ipv6 router ospf 1
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#exit
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ipv6 ospf 1 area 0
R2(config-if)#exit
R2(config)#
*Sep 12 03:04:56.803: %OSPFv3-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial1/0 from LOADING to FULL, Loading Doner
R2(config)#
R2(config)#interface serial 1/1
R2(config-if)#ipv6 ospf 1 area 1
R2(config-if)#exit
R2(config)#
```

批注 [stanley454]：配置 S1/0 接口从属于 AREA 0。

批注 [stanley455]：配置 S1/1 接口从属于 AREA 1。

3、查看 R2 路由器邻居表：

```
R2#show ipv6 ospf neighbor detail
 Neighbor 1.1.1.1
    In the area 0 via interface Serial1/0
    Neighbor: interface-id 4, link-local address FE80::C800:EFF:FEAC:0
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x6408C935
    Dead timer due in 00:00:38
    Neighbor is up for 00:02:41
    Index 1/1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 3.3.3.3
    In the area 1 via interface Serial1/1
    Neighbor: interface-id 3, link-local address FE80::C802:EFF:FEAC:0
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x64070B61
    Dead timer due in 00:00:36
    Neighbor is up for 00:00:13
    Index 1/1/2, retransmission queue length 0, number of retransmission 1
```

```
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
R2#
```

4、查看 R3 的 OSPFv3 链路状态数据库：

```
R3#show ipv6 ospf database

            OSPFv3 Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 1)
ADV Router      Age         Seq#       Fragment ID  Link count  Bits
2.2.2.2         86          0x80000002 0            1           B
3.3.3.3         86          0x80000002 0            1           None

                Inter Area Prefix Link States (Area 1)
ADV Router      Age         Seq#       Prefix
2.2.2.2         227         0x80000001 2001:AB1:0:2::/64
2.2.2.2         227         0x80000001 2001:AB1:0:8::/64
2.2.2.2         227         0x80000001 2001:AB1:0:9::/64
2.2.2.2         227         0x80000001 2001:AB1:0:A::/64
2.2.2.2         227         0x80000001 2001:AB1:0:B::/64

                Link (Type-8) Link States (Area 1)
ADV Router      Age         Seq#       Link ID    Interface
2.2.2.2         226         0x80000001 4          Se1/0
3.3.3.3         86          0x80000001 3          Se1/0

                Intra Area Prefix Link States (Area 1)
ADV Router      Age         Seq#       Link ID    Ref-lstype  Ref-LSID
2.2.2.2         226         0x80000001 0          0x2001      0
3.3.3.3         87          0x80000002 0          0x2001      0
R3#
```

批注 [stanley456]:
LSA 0X2003 与 OSPFv2 的 LSA3 类似，主要用于通告区域间的前缀信息。
其泛洪范围为整个 AS。

5、使用 ping 命令确认路由有效性；

```
R3#ping 2001:ab1:0:8::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:8::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/61/68 ms
R3#
```

6、查看 R3 的路由表：

```
R3#show ipv6 route
```

```
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI  2001:AB1:0:2::/64 [110/128]
     via FE80::C801:EFF:FEAC:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
OI  2001:AB1:0:8::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
OI  2001:AB1:0:9::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
OI  2001:AB1:0:A::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
OI  2001:AB1:0:B::/64 [110/129]
     via FE80::C801:EFF:FEAC:0, Serial1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R3#
```

批注 [stanley457]: 由 LSA 0X2003 学习到的区域间路由信息。

7、在 R2 路由器上配置区域汇总，减小路由表大小，提高路由效率：

```
R2(config)#
R2(config)#ipv6 router ospf 1
R2(config-rtr)#area 0 range 2001:ab1:0:8::/62
R2(config-rtr)#
```

批注 [stanley458]: 对区域 0 进行手工汇总配置。

8、再次查看 R3 路由器的路由表，确认手工区域汇总：

```
R3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
OI   2001:AB1:0:2::/64 [110/128]
      via FE80::C801:EFF:FEAC:0, Serial1/0
C    2001:AB1:0:3::/64 [0/0]
      via ::, Serial1/0
L    2001:AB1:0:3::2/128 [0/0]
      via ::, Serial1/0
C    2001:AB1:0:4::/64 [0/0]
      via ::, Loopback0
L    2001:AB1:0:4::1/128 [0/0]
      via ::, Loopback0
OI   2001:AB1:0:8::/62 [110/129]
      via FE80::C801:EFF:FEAC:0, Serial1/0
L    FE80::/10 [0/0]
      via ::, Null0
L    FF00::/8 [0/0]
      via ::, Null0
R3#
```

批注 [stanley459]: 此条路由说明手工区域汇总成功。

9、实验完成。

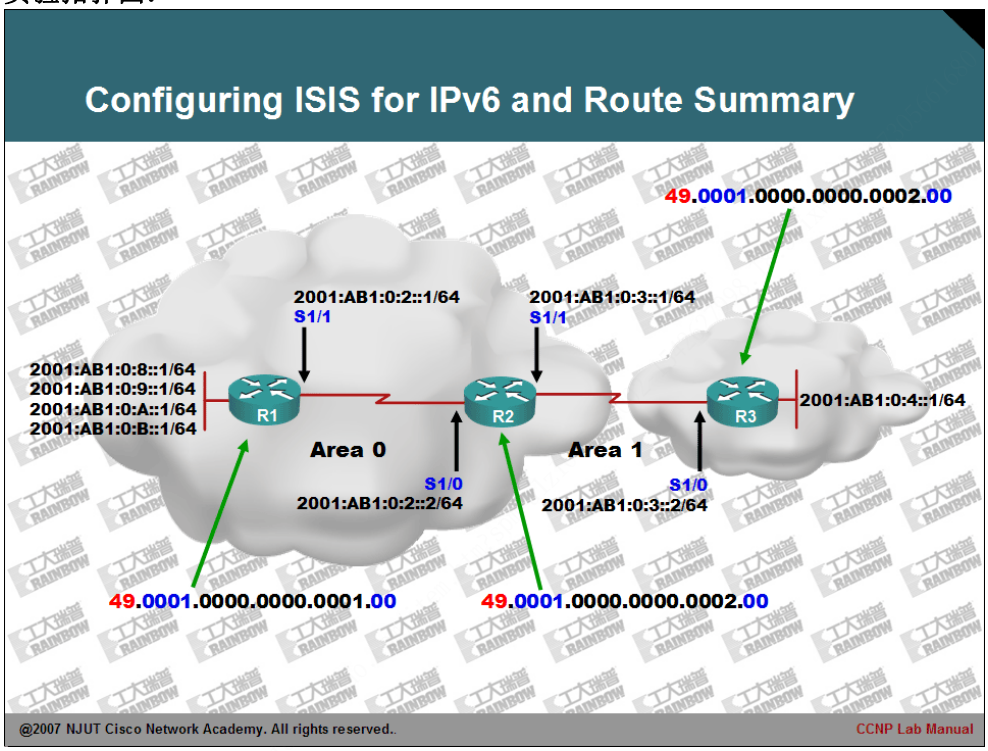
CCNP Lab Manual

Lab 49. Configuring ISIS for IPv6 and Route Summary

实验目的：

1、掌握基于 IPv6 的 ISIS 路由协议的配置。
2、掌握 IPv6 ISIS 的路由汇总配置。
3、了解 ISIS 单拓扑到多拓扑迁移功能。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IPv6 地址，并且使用 ping 命令确认直连接口的互通性。

2、分别在 R1，R2 和 R3 路由器上配置 ISIS for IPv6 协议。配置如下：

```
R1(config)#router isis wy_ipv6_isis
R1(config-router)#net 49.0001.0000.0000.0001.00
R1(config-router)#exit
R1(config)#
R1(config)#interface serial 1/1
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 router isis wy_ipv6_isis
R1(config-if)#exit
R1(config)#
R1(config)#interface loopback 0
R1(config-if)#ipv6 router isis wy_ipv6_isis
R1(config-if)#exit
R1(config)#
```

批注 [stanley460]：全局启用 ISIS 路由进程。

批注 [stanley461]：接口下启用 IPv6。此条命令为可选配置。

批注 [stanley462]：将接口加入到 wy_ipv6_isis 的 ISIS 路由进程域。

```
R2(config)#router isis wy_ipv6_isis
R2(config-router)#net 49.0001.0000.0000.0002.00
R2(config-router)#exit
R2(config)#
R2(config)#interface serial 1/0
R2(config-if)#ipv6 router isis wy_ipv6_isis
R2(config-if)#exit
R2(config)#
R2(config)#interface serial 1/1
R2(config-if)#ipv6 router isis wy_ipv6_isis
R2(config-if)#exit
R2(config)#exit
R2#
```

```
R3(config)#router isis wy_ipv6_isis
R3(config-router)#net 49.0002.0000.0000.0003.00
R3(config-router)#exit
R3(config)#
R3(config)#interface serial 1/0
R3(config-if)#ipv6 router isis wy_ipv6_isis
R3(config-if)#exit
R3(config)#
R3(config)#interface loopback 0
R3(config-if)#ipv6 router isis wy_ipv6_isis
```

```
R3(config-if)#exit
```

3、在 R2 路由器上查看 ISIS 的邻居关系：

```
R2#show isis neighbors

System Id      Type Interface IP Address      State Holdtime Circuit Id
R3             L2   Se1/1                     UP    27       00
R1             L2   Se1/0                     UP    28       00
R2#
```

4、在 R2 上查看更为详细的 ISIS 邻居关系信息：

```
R2#show clns is-neighbors detail

System Id      Interface   State  Type Priority  Circuit Id         Format
R3             Se1/1       Up     L2   0         00                 Phase V
  Area Address(es): 49.0002
  IPv6 Address(es): FE80::C802:DFF:FE30:0
  Uptime: 00:01:27
  NSF capable
R1             Se1/0       Up     L2   0         00                 Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::C800:DFF:FE30:0
  Uptime: 00:05:17
  NSF capable
R2#
```

批注 [stanley463]: 区域信息

批注 [stanley464]: 用于 IPv6 的 ISIS 更新源地址。

5、在 R2 上查看 ISIS 的数据库：

```
R2#show isis database verbose level-1

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R2.00-00            * 0x00000004   0xC0A1        757               1/0/0
  Area Address: 29.0001
  NLPID:        0x8E
  Hostname: R2
  IPv6 Address: 2001:AB1:0:3::1
  Metric: 10         IPv6 2001:AB1:0:2::/64
  Metric: 10         IPv6 2001:AB1:0:3::/64
R2#
R2#show isis database verbose level-2

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
R1.00-00              0x00000004   0x649F        665               0/0/0
  Area Address: 49.0001
```

批注 [stanley465]: 查看 level-1 的数据库信息。

批注 [stanley466]: 两个直连网络的路由信息。

批注 [stanley467]: 查看 level-2 的数据库信息。

```
  NLPID:         0x8E
  Hostname: R1
  IPv6 Address: 2001:AB1:0:8::1
  IPv6 Address: 2001:AB1:0:9::1
  IPv6 Address: 2001:AB1:0:A::1
  IPv6 Address: 2001:AB1:0:B::1
  Metric: 10         IS R2.00
  Metric: 10         IPv6 2001:AB1:0:2::/64
  Metric: 10         IPv6 2001:AB1:0:8::/64
  Metric: 10         IPv6 2001:AB1:0:9::/64
  Metric: 10         IPv6 2001:AB1:0:A::/64
  Metric: 10         IPv6 2001:AB1:0:B::/64
R2.00-00            * 0x00000005   0x54E3        896              0/0/0
  Area Address: 49.0001
  NLPID:         0x8E
  Hostname: R2
  IPv6 Address: 2001:AB1:0:3::1
  Metric: 10         IS R3.00
  Metric: 10         IS R1.00
  Metric: 10         IPv6 2001:AB1:0:2::/64
  Metric: 10         IPv6 2001:AB1:0:3::/64
R3.00-00             0x00000004   0x307B        898              0/0/0
  Area Address: 49.0002
  NLPID:         0x8E
  Hostname: R3
  IPv6 Address: 2001:AB1:0:4::1
  Metric: 10         IS R2.00
  Metric: 10         IPv6 2001:AB1:0:3::/64
  Metric: 10         IPv6 2001:AB1:0:4::/64
R2#
```

批注 [stanley468]: R1 路由器相关路由信息。

6、查看 R3 路由器的路由表：

```
R3#show ipv6 route
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I2  2001:AB1:0:2::/64 [115/20]
     via FE80::C801:DFF:FE30:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
```

```
     via ::, Serial1/0
C    2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L    2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
I2   2001:AB1:0:8::/64 [115/30]
     via FE80::C801:DFF:FE30:0, Serial1/0
I2   2001:AB1:0:9::/64 [115/30]
     via FE80::C801:DFF:FE30:0, Serial1/0
I2   2001:AB1:0:A::/64 [115/30]
     via FE80::C801:DFF:FE30:0, Serial1/0
I2   2001:AB1:0:B::/64 [115/30]
     via FE80::C801:DFF:FE30:0, Serial1/0
L    FE80::/10 [0/0]
     via ::, Null0
L    FF00::/8 [0/0]
     via ::, Null0
R3#
```

7、使用 ping 命令确认路由有效性：

```
R3#ping 2001:ab1:0:8::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:8::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/129/144 ms
R3#
```

8、再次查看 R1 路由表信息：

```
R1#show ipv6 route isis
IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I1   2001:AB1:0:3::/64 [115/20]
     via FE80::C801:DFF:FE30:0, Serial1/1
I2   2001:AB1:0:4::/64 [115/30]
     via FE80::C801:DFF:FE30:0, Serial1/1
R1#
```

9、在 R1 上配置 ISIS 的类型：

```
R1(config)#router isis wy_ipv6_isis
R1(config-router)#is-type level-1
```

批注 [stanley469]：将 IS 类型修改为 level-1。

```
R1(config-router)#exit
```

10、再次查看 R1 路由器的路由表信息：

```
R1#show ipv6 route isis
IPv6 Routing Table - 14 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I1  ::/0 [115/10]
     via FE80::C801:DFF:FE30:0, Serial1/1
I1  2001:AB1:0:3::/64 [115/20]
     via FE80::C801:DFF:FE30:0, Serial1/1
```

批注 [stanley470]：通过修改R1路由器的中间系统类型，可以看出此时对于非本区域的路由，采用了默认路由描述。其与 IPv4 ISIS 路由协议类似。

11、在 R2 上配置针对 49.0001 区域的路由总结，：

```
R2(config)#router isis wy_ipv6_isis
R2(config-router)#
R2(config-router)#address-family ipv6
R2(config-router-af)#
R2(config-router-af)#summary-prefix 2001:ab1:0:8::/62
R2(config-router-af)#exit
R2(config-router)#exit
```

批注 [stanley471]：进入IPv6 地址家族配置模式。

批注 [stanley472]：配置手工区域路由总结。

12、再次查看 R3 路由表信息，并与第 6 步的 R3 路由表进行比较：

```
R3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
I2  2001:AB1:0:2::/64 [115/20]
     via FE80::C801:DFF:FE30:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
I2  2001:AB1:0:8::/62 [115/30]
     via FE80::C801:DFF:FE30:0, Serial1/0
L   FE80::/10 [0/0]
```

批注 [stanley473]：R1 路由器上的回环口路由，由一条汇总路由所描述。

```
     via ::, Null0
L    FF00::/8 [0/0]
     via ::, Null0
```

13、如果网络设计要求两种 IP 协议独立地运行，你可以将 ISIS 迁移到多拓扑模式，这样更有利于对独立的协议的针对性优化调整。具体配置如下：

```
R1(config)#router isis wy_ipv6_isis
R1(config-router)#metric-style wide transition
R1(config-router)#address-family ipv6
R1(config-router-af)#multi-topology transition
R1(config-router-af)#exit
R1(config-router)#exit
```

批注 [stanley474]：配置拓扑模式下度量的迁移。

批注 [stanley475]：针对 IPv6 配置多拓扑模式。

14、当 ISIS 路由协议工作在多拓扑模式下，你能够独立于 IPv4 度量来设置 IPv6 的度量，配置如下：

```
R1(config)#interface serial 1/1
R1(config-if)#
R1(config-if)#isis metric 20
R1(config-if)#
R1(config-if)#isis ipv6 metric 100
R1(config-if)#
R1(config-if)#exit
```

批注 [stanley476]：如果工作在单拓扑模式下，此配置命令，将会影响 IPv4 和 v6 的 ISIS 度量计算。

批注 [stanley477]：当 ISIS 工作于多拓扑模式下，此配置命令仅仅针对于 IPv6 的 ISIS 的路由协议的度量计算。而独立于其它协议家族。

15、实验完成。

CCNP Lab Manual

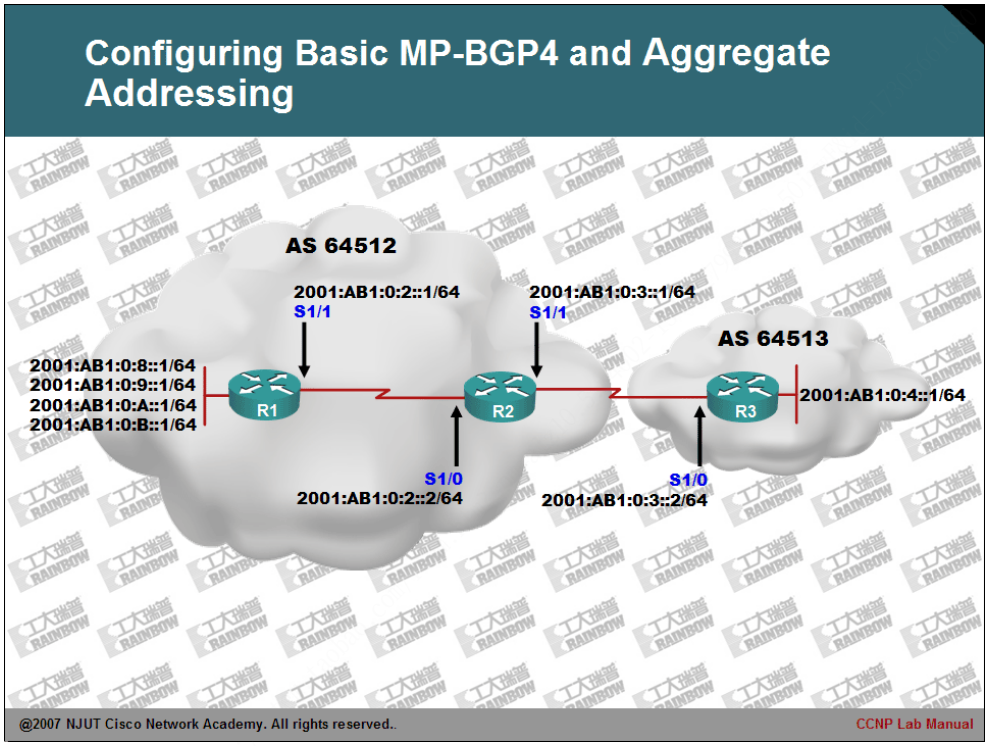
Lab 50. Configuring Basic MP-BGP4 and Aggregate Addressing

实验目的：

1、掌握基于 IPv6 的 MP-BGP4 配置。

2、配置 MP-BGP4 地址聚合。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IPv6 地址，并且使用 ping 命令确认直连接口的互通性。

2、根据拓扑在三台路由器上配置 MP-BGP4 路由协议，具体配置如下所示：

```
R1(config)#
R1(config)#router bgp 64512
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#
R1(config-router)#neighbor 2001:ab1:0:2::2 remote-as 64512
R1(config-router)#
R1(config-router)#no synchronization
R1(config-router)#
R1(config-router)#address-family ipv6
R1(config-router-af)#
R1(config-router-af)#neighbor 2001:ab1:0:2::2 activate
R1(config-router-af)#net
R1(config-router-af)#network 2001:ab1:0:8::0/64
R1(config-router-af)#network 2001:ab1:0:9::0/64
R1(config-router-af)#network 2001:ab1:0:a::0/64
R1(config-router-af)#network 2001:ab1:0:b::0/64
R1(config-router-af)#network 2001:ab1:0:2::/64
R1(config-router-af)#exit
R1(config-router)#exit
R1(config)#
```

批注 [stanley478]： 为 BGP 指定 RouterID。虽然 MP-BGP4 可以为 IPv6 提供路由。但其仍然需要一个 32 位长度的 RouterID。如果不配置则会导致 BGP 邻居关系无法创建。

如果不采用手工配置，也可以为本地路由器配置一个 IPv4 地址的环回接口。

批注 [stanley479]： 配置 BGP 的邻居对等体。

批注 [stanley480]： 进入 IPv6 地址簇。

批注 [stanley481]： 在 IPv6 地址簇下激活邻居对等体关系。

批注 [stanley482]： 宣告需要发布的 IPv6 地址前缀。

```
R2(config)#
R2(config)#router bgp 64512
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 2001:ab1:0:2::1 remote-as 64512
R2(config-router)#neighbor 2001:ab1:0:3::2 remote-as 64513
R2(config-router)#
R2(config-router)#address-family ipv6
R2(config-router-af)#neighbor 2001:ab1:0:2::1 activate
R2(config-router-af)#neighbor 2001:ab1:0:3::2 activate
R2(config-router-af)#network 2001:ab1:0:2::/64
R2(config-router-af)#network 2001:ab1:0:3::/64
R2(config-router-af)#exit
R2(config-router)#no synchronization
R2(config-router)#exit
R2(config)#exit
R2#
```

```
R3(config)#router bgp 64513
R3(config-router)#bgp router-id 3.3.3.3
R3(config-router)#neighbor 2001:ab1:0:3::1 remote-as 64512
R3(config-router)#address-family ipv6
R3(config-router-af)#neighbor 2001:ab1:0:3::1 activate
R3(config-router-af)#network  2001:ab1:0:4::/64
R3(config-router-af)#network  2001:ab1:0:3::/64
R3(config-router-af)#exit
R3(config-router)#exit
R3(config)#
```

3、在 R2 上查看 MP-BGP4 邻居关系：

```
R2#show bgp summary
BGP router identifier 2.2.2.2, local AS number 64512
BGP table version is 7, main routing table version 7
6 network entries using 798 bytes of memory
7 path entries using 504 bytes of memory
3 BGP path attribute entries using 180 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1506 total bytes of memory
BGP activity 7/1 prefixes, 8/1 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:AB1:0:2::1 4 64512      12      14        7    0    0 00:06:18        5
2001:AB1:0:3::2 4 64513       6       7        7    0    0 00:01:23        2
R2#
```

批注 [stanley483]：手工为 BGP 配置的 RouterID。

批注 [stanley484]：邻居对等体关系成功创建。

4、查看 MP-BGP4 的 IPv6 数据库：

```
R2#show bgp ipv6
BGP table version is 16, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i2001:AB1:0:2::/64
                    2001:AB1:0:2::1          0    100      0 i
*>                  ::                       0         32768 i
*  2001:AB1:0:3::/64
                    2001:AB1:0:3::2          0             0 64513 i
*>                  ::                       0         32768 i
*> 2001:AB1:0:4::/64
```

```
                    2001:AB1:0:3::2          0              0 64513 i
*>i2001:AB1:0:8::/64
                    2001:AB1:0:2::1          0    100       0 i
*>i2001:AB1:0:9::/64
                    2001:AB1:0:2::1          0    100       0 i
*>i2001:AB1:0:A::/64
                    2001:AB1:0:2::1          0    100       0 i
*>i2001:AB1:0:B::/64
                    2001:AB1:0:2::1          0    100       0 i
R2#
```

5、查看 R3 的 IPv6 路由表：

```
R3#show ipv6 route
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:AB1:0:2::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
B   2001:AB1:0:8::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:9::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:A::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:B::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R3#
```

6、在 R2 路由器上配置路由聚合：

```
R2(config)#router bgp 64512
R2(config-router)#address-family ipv6
R2(config-router-af)#aggregate-address 2001:ab1:0:8::/62 summary-only
R2(config-router-af)#exit
R2(config-router)#
```

批注 [stanley485]：配置地址聚合。使用 summary-only 指定仅发送聚合路由。

7、再次查看 R3 路由表，确认聚合路由：

```
R3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:AB1:0:2::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
C   2001:AB1:0:3::/64 [0/0]
     via ::, Serial1/0
L   2001:AB1:0:3::2/128 [0/0]
     via ::, Serial1/0
C   2001:AB1:0:4::/64 [0/0]
     via ::, Loopback0
L   2001:AB1:0:4::1/128 [0/0]
     via ::, Loopback0
B   2001:AB1:0:8::/62 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R3#
```

批注 [stanley486]：被聚合的路由。

8、在 R3 路由器上查看聚合路由属性：

```
R3#show bgp ipv6 2001:ab1:0:8::/62
BGP routing table entry for 2001:AB1:0:8::/62, version 22
Paths: (1 available, best #1, table Global-IPv6-Table)
  Not advertised to any peer
  64512, (aggregated by 64512 2.2.2.2)
    2001:AB1:0:3::1 from 2001:AB1:0:3::1 (2.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, external, atomic-aggregate, best
R3#
```

批注 [stanley487]：显示了聚合者为 64512 自治系统的 RouterID 为 2.2.2.2 路由器。

9、在 R3 路由器使用 ping 命令确认路由有效性：

```
R3#ping
R3#ping 2001:ab1:0:8::1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:8::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/76/96 ms
R3#
R3#ping 2001:ab1:0:b::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:AB1:0:B::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/94/128 ms
R3#
```

10、实验完成。

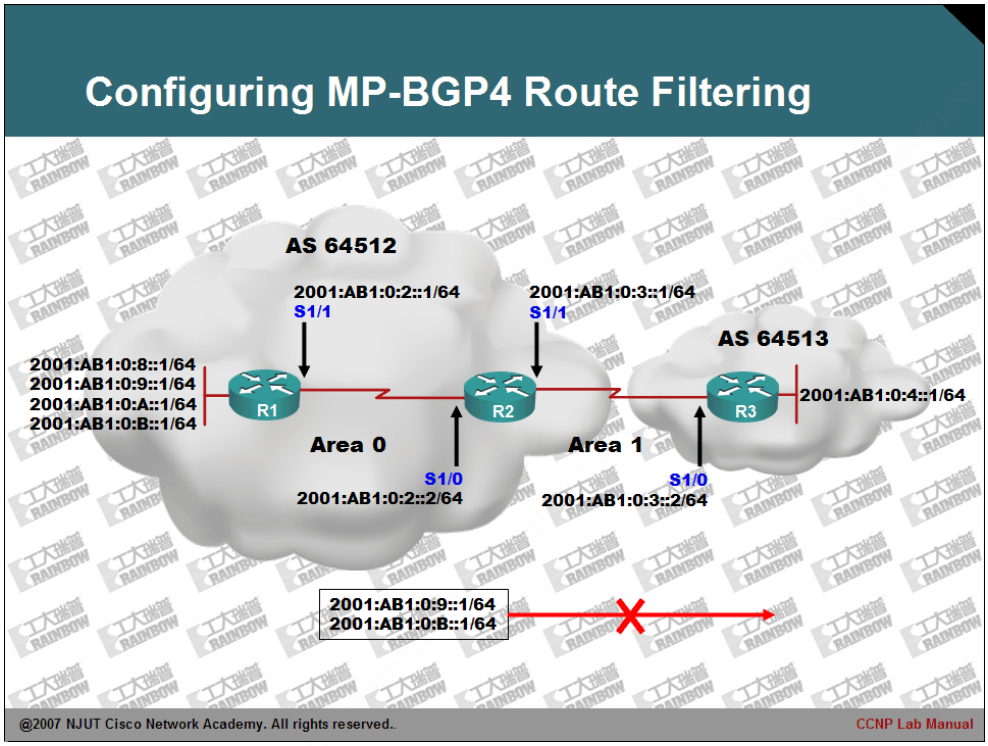
Lab 51. Configuring MP-BGP4 Route Filtering

实验目的：

1、配置基于 IPv6 的访问管制列表。

2、配置路由图实现 MP-BGP4 的路由过滤。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IPv6 地址，并且使用 ping 命令确认直连接口的互通性。

2、配置各台路由器的 MP-BGP4 路由协议，并且使用相关命令确认 MP-BGP4 工作正常。

3、根据拓扑要求，64512 自治系统中的 2001:AB1:0:9::/64 和 2001:AB1:0:B::/64 两个网络前缀不允许被发布给 64513 的自治系统。

4、首先查看 R3 路由器路由表信息：

```
R3#show ipv6 route bgp
IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:AB1:0:2::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:8::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:9::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:A::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:B::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
R3#
```

4、在 R2 路由器上配置 ACL 标识需要过滤的两个网络前缀。如下所示：

```
R2(config)#ipv6 access-list block_prefix
R2(config-ipv6-acl)#
R2(config-ipv6-acl)#permit ipv6 2001:ab1:0:9::/64 any
R2(config-ipv6-acl)#permit ipv6 2001:ab1:0:b::/64 any
R2(config-ipv6-acl)#
R2(config-ipv6-acl)#exit
```

批注 [stanley488]：创建名称为 block_prefix 的 IPv6 的访问控制列表。

批注 [stanley489]：标识需要被过滤的网络前缀。

5、配置路由图引用之前创建的访问控制列表：

```
R2(config)#route-map bgp_filter deny 10
R2(config-route-map)#
R2(config-route-map)#match ipv6 address block_prefix
R2(config-route-map)#
R2(config-route-map)#exit
R2(config)#
```

批注 [stanley490]：创建路由图。并且设置其动作为 deny。

批注 [stanley491]：引用之前配置的访问控制列表。

```
R2(config)#route-map bgp_filter permit 20
R2(config-route-map)#exit
R2(config)#
```

批注 [stanley492]：对于其它的网络前缀设置允许转发。

6、在 MP-BGP4 中配置路由过滤，命令如下所示：

```
R2(config)#router bgp 64512
R2(config-router)#
R2(config-router)#address-family ipv6
R2(config-router-af)#
R2(config-router-af)#neighbor 2001:ab1:0:3::2 route-map bgp_filter out
R2(config-router-af)#
R2(config-router-af)#exit
R2(config-router)#exit
```

批注 [stanley493]：针对 R3 对等体实施路由过滤。

7、再次查看 R3 路由器路由表，确认路由过滤：

```
R3#
R3#show ipv6 route bgp
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:AB1:0:2::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:8::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
B   2001:AB1:0:A::/64 [20/0]
     via FE80::C801:DFF:FEE8:0, Serial1/0
R3#
```

批注 [stanley494]：此时 R3 路由器已经无法学习到被过滤的网络前缀。

8、实验完成。

CCNP Lab Manual

Building Cisco Multilayer Switched Networks

CCNP Lab Manual

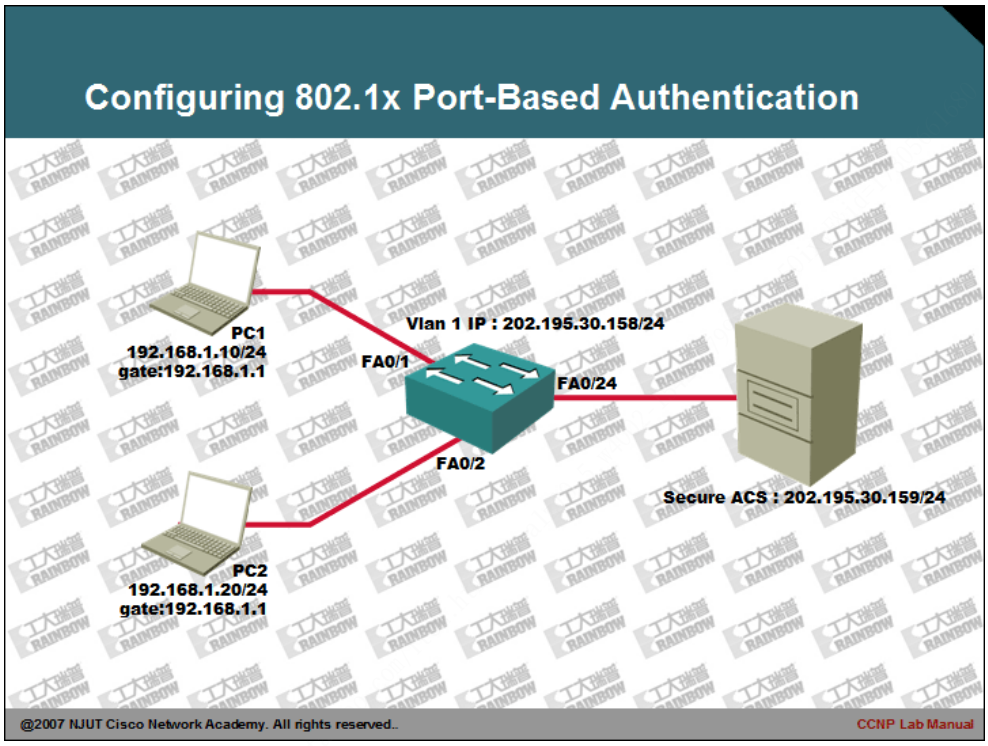
Lab 52. Configuring 802.1x Port-Based Authentication

实验目的：

1、掌握基于端口的 802.1x 配置方法。

2、掌握 Cisco TACACS+ 服务器认证服务器配置。

实验拓扑图：

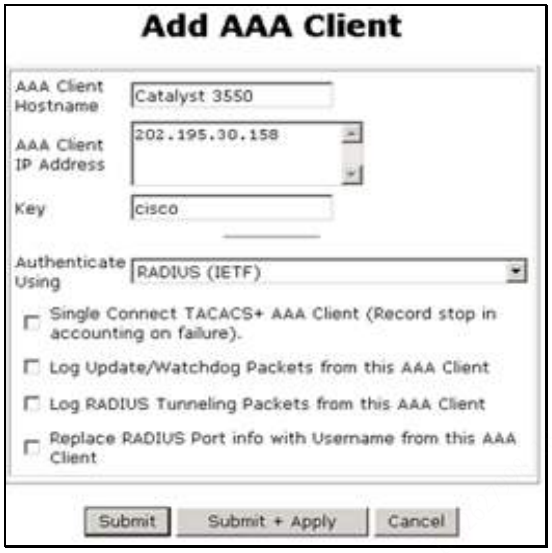


实验步骤及要求：

1、安装 ACS 服务器的 Java 环境，建议使用 j2re-1_4_2_10-windows-i586-p.exe。

2、安装 ACS 软件，本实验使用的是 Cisco secure ACS 4.0 版本。

3、配置 ACS 服务器与 Catalyst 3550 交换机的通信，在 ACS 服务器上点击“Network Configuration”，选择添加一个 AAA 用户。其中 Key 为 ACS 与 3550 交换机进行了进行通信验证使用，双方必须密码匹配。认证协议使用 Radius(IETF)：



4、配置 IETF 的组属性。点击“Interface Configuration”，选择“RADIUS (IETF)”，确认并选中如下三个选项，并按下 submit 按钮。

```
[064] Tunnel-Type
[065] Tunnel-Medium-Type
[081] Tunnel-Private-Group-ID
```

5、创建一个 802.1x 的用户帐号。点击<User Configuration>，输入新建的帐号名 stanley，并点击 Add/Edit 按钮，在<User Setup>中，输入用户 stanley 的帐号的密码。并将此帐号指定到 Group 1。也可以指定其它的组，并点击 Submit 按钮：

6、配置 Group 组属性。点击“Group Configuration”，选择“Group 1”，点击“Edit Settings”。选中：

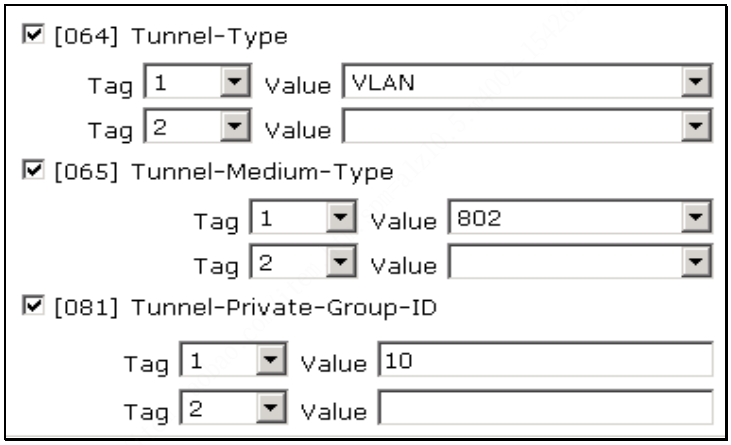
[064]Tunnel-Type，并编辑 Tag 1 的 Value 为 VLAN，
[065]Tunnel-Medium-Type，并设置 Tag1 的 Value 为 802，
[081]Tunnel-Private-Group-ID 的 Tag 1 的 Value 为 10。

批注 [s495]：设置对 Group 1 的用户的 VLAN 进行配置。

批注 [s496]：配置类型为 802，即 802.1x 的协议类型

批注 [s497]：配置 Group 1 的用户连入网络后，认证通过后，将从属于 Vlan 10。

然后击 Submit + Restart 按扭：



7、采用相同的方法创建用户帐号 steve 密码为 cisco，并且属于 Group 2。同时指定 Group 2 的属性为：

[064]Tunnel-Type，并编辑 Tag 1 的 Value 为 VLAN
[065]Tunnel-Medium-Type，并设置 Tag1 的 Value 为 802
[081]Tunnel-Private-Group-ID 的 Tag 1 的 Value 为 20

8、配置 ACS 服务器，点击“System Configurateion”，点击“Global Authentication Setup”，将 LEAP 的“Allow LEAP (For Aironet only)”打勾

批注 [stanley498]：如果不配置此项。会导致 ACS 的认证失败。

去掉。并点击 Submit + Restart：

9、配置 3550 交换机的 Vlan 1 的 IP。交换机使用此 IP 与 ACS 服务器进行通信。并使用 ping 命令确认是否能够 ping 通 ACS 服务器。

```
3550(config)#
3550(config)#interface vlan 1
3550(config-if)#ip address 202.195.30.158 255.255.255.0
3550(config-if)#no shutdown
3550(config-if)#exit
3550(config)#
```

批注 [s499]：此地址为步骤三中所有设置的 AAA 客户端的地址。

10、在 3550 上创建 VLAN：

```
3550(config)#vlan 10
3550(config-vlan)#exit
3550(config)#vlan 20
3550(config-vlan)#exit
```

11、配置 3550 的 AAA：

```
3550(config)#aaa new-model

3550(config)#radius-server host 202.195.30.159 key cisco

3550(config)#radius-server vsa send

3550(config)#aaa authentication login default none

3550(config)#aaa authentication dot1x default group radius

3550(config)#aaa authorization network default group radius

3550(config)#dot1x system-auth-control
```

批注 [s500]：启用 AAA

批注 [s501]：配置 Radius 服务器，并指定通信密钥

批注 [s502]：向 Radius 服务器发送 CISCO 私有属性集。

批注 [s503]：设置不对 login 进行认证。会防止与 ACS 通信失败后，无法登录到本地交换机。

批注 [s504]：设置使用 Radius 服务器进行配置 DOT1X。

批注 [s505]：设置使用 Radius 服务器进行授权

批注 [s506]：启用 DOT1X 的认证控制。

12、配置 3550 的交换机接口：

```
3550(config)#interface range fastEthernet 0/1 - 20
3550(config-if-range)#switchport mode access
3550(config-if-range)#spanning-tree portfast
3550(config-if-range)#dot1x port-control auto
3550(config-if-range)#exit
```

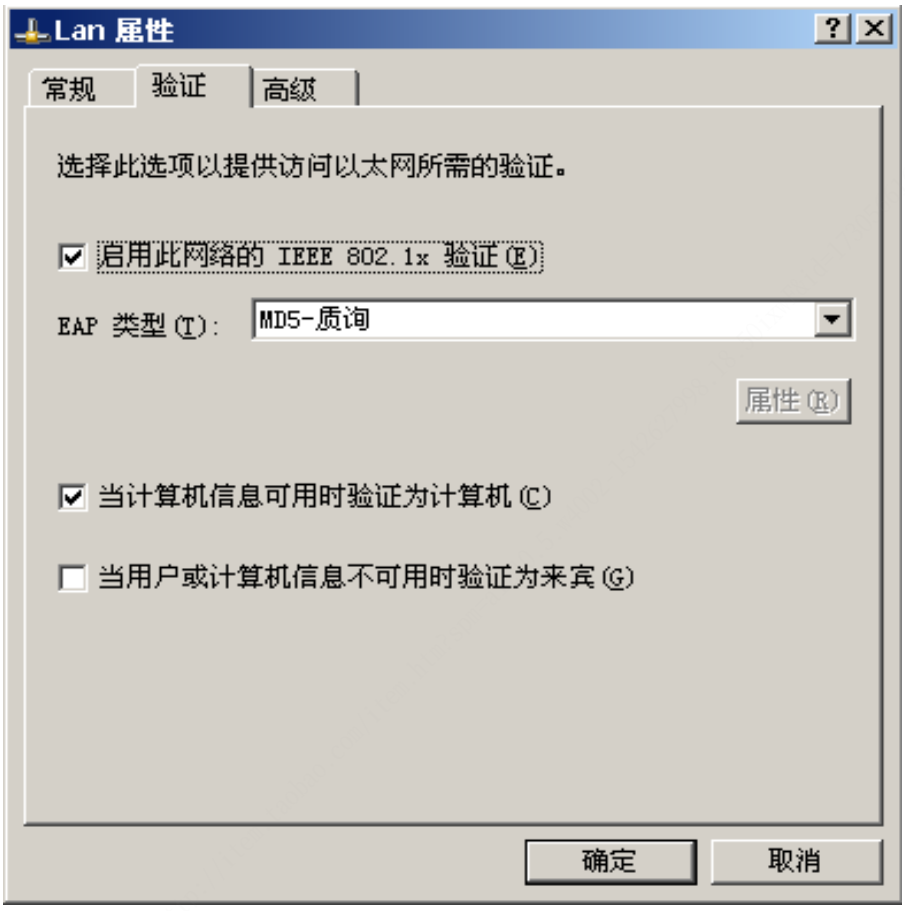
批注 [s507]：配置 fa0/1 - 20 接口启用 DOT1X

13、查看 3550 的交换机的 VLAN 配置：

```
3550#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
```

```
                                          Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                          Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                          Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                          Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                          Gi0/1, Gi0/2
10   VLAN0010                 active
20   VLAN0010                 active
3550#
```

14、设置客户端的网卡的验证，启用 IEEE 802.1x 的验证，并选择的 EAP 的类型为 MD5-质询的方式。点击确定：



15、将 R1 和 R2 客户端的网卡连线到 3550 交换机的 FastEthernet 0/1 接口后。Windows 系统会弹出 802.1X 的认证登录对话框。在此输入 802.1x 的帐号和密码。(Stanley/cisco)：

16、当双方主机认证成功后，再次查看 3550 交换机的 VLAN 信息：

```
3550#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6,
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10,
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14,
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18,
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22,
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2

10   VLAN0010                         active    Fa0/1
20   VLAN0020                         active    Fa0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
3550#
```

17、实验完成。

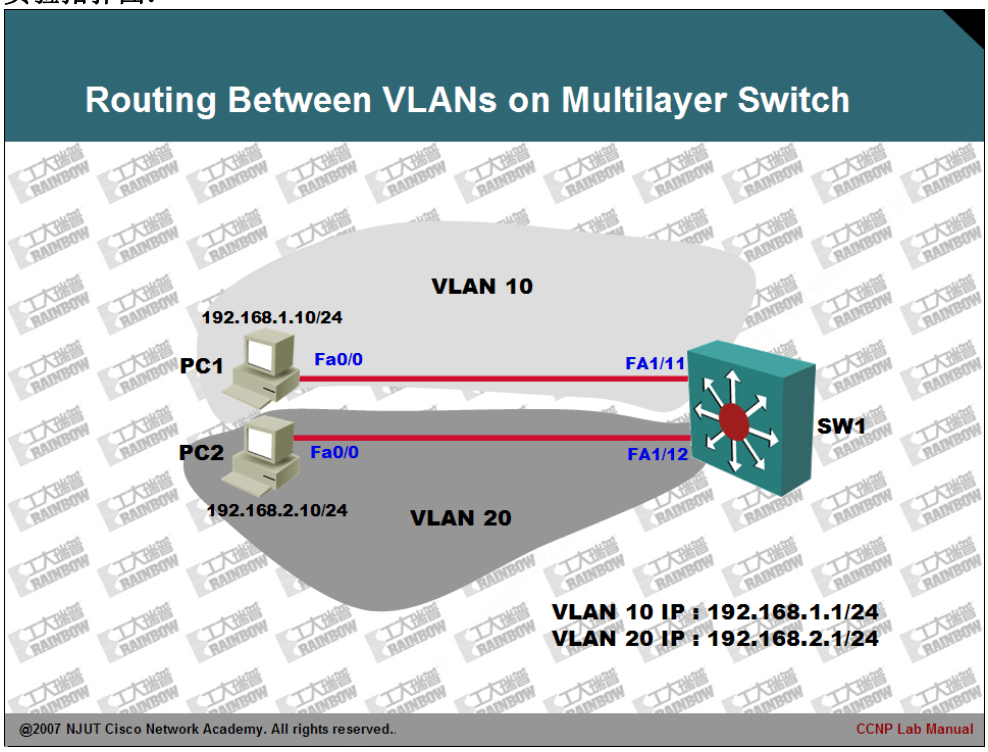
CCNP Lab Manual

Lab 53. Routing Between VLANs on Multilayer Switch

实验目的：

1、掌握基于多层交换的 VLAN 间路由的配置。

实验拓扑图：



实验步骤及要求：

1、首先配置 PC1 和 PC2 主机地址，本实验使用了两台路由器模拟 PC 主机。

2、配置如下所示：

```
PC1(config)#interface fastethernet 0/0
PC1(config-if)#ip address 192.168.1.10 255.255.255.0
PC1(config-if)#no shutdown
PC1(config-if)#exit
PC1(config)#
PC1(config)#no ip routing
PC1(config)#
PC1(config)#ip default-gateway 192.168.1.1
```

批注 [stanley508]：关闭路由器的三层路由功能。

批注 [stanley509]：为路由器配置默认网关。

```
PC2(config)#interface fastethernet 0/0
PC2(config-if)#ip address 192.168.2.10 255.255.255.0
PC2(config-if)#no shutdown
PC2(config-if)#exit
PC2(config)#
PC2(config)#no ip routing
PC2(config)#
PC2(config)#ip default-gateway 192.168.2.1
```

3、在交换机上配置 VLAN，同时将连接到客户端的端口按拓扑分入不同的 VLAN 中，配置如下：

```
SW1(config)#vlan 10
SW1(config-vlan)#name cisco
SW1(config-vlan)#exit
SW1(config)#
SW1(config)#vlan 20
SW1(config-vlan)#name Microsoft
SW1(config-vlan)#exit
SW1(config)#
SW1(config)#interface fastethernet 1/11
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
SW1(config)#
SW1(config)#inter fastEthernet 1/12
SW1(config-if)#switchport access vlan 20
SW1(config-if)#exit
SW1(config)#
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
```

批注 [stanley510]：全局配置模式下创建 VLAN 10。

批注 [stanley511]：为 VLAN 配置一个好记的名称。

批注 [stanley512]：将接口加入到 VLAN。

批注 [stanley513]：启用交换机的 VLAN 10 的 SVI 接口。

批注 [stanley514]：为 VLAN1 的 SVI 接口配置 IP 地址，其将用于 PC1 的默认网关。

```
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#
SW1(config)#interface vlan 20
SW1(config-if)#ip address 192.168.2.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#
SW1(config)#ip routing
SW1(config)#
```

批注 [stanley515]：启用交换机的三层路由功能。

4、查看 SW1 交换机的 VLAN 配置，确认 VLAN：

```
SW1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/13
                                                Fa1/14, Fa1/15
10   cisco                            active    Fa1/11
20   microsoft                        active    Fa1/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
SW1#
```

批注 [stanley516]：配置的 VLAN 信息。

5、在 PC1 或 PC2 上使用 ping 命令确认 VLAN 间是否可以相互访问：

```
PC1#
PC1#ping 192.168.2.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/57/96 ms
PC1#
```

批注 [stanley517]：结果显示 VLAN 间路由配置成功。

6、在交换机上查看路由表：

```
SW1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Vlan10
C    192.168.2.0/24 is directly connected, Vlan20
SW1#
```

批注 [stanley518]：到达客户端网络的路由条目，其出口为本地址的 SVI 接口。

7、实验完成。

CCNP Lab Manual

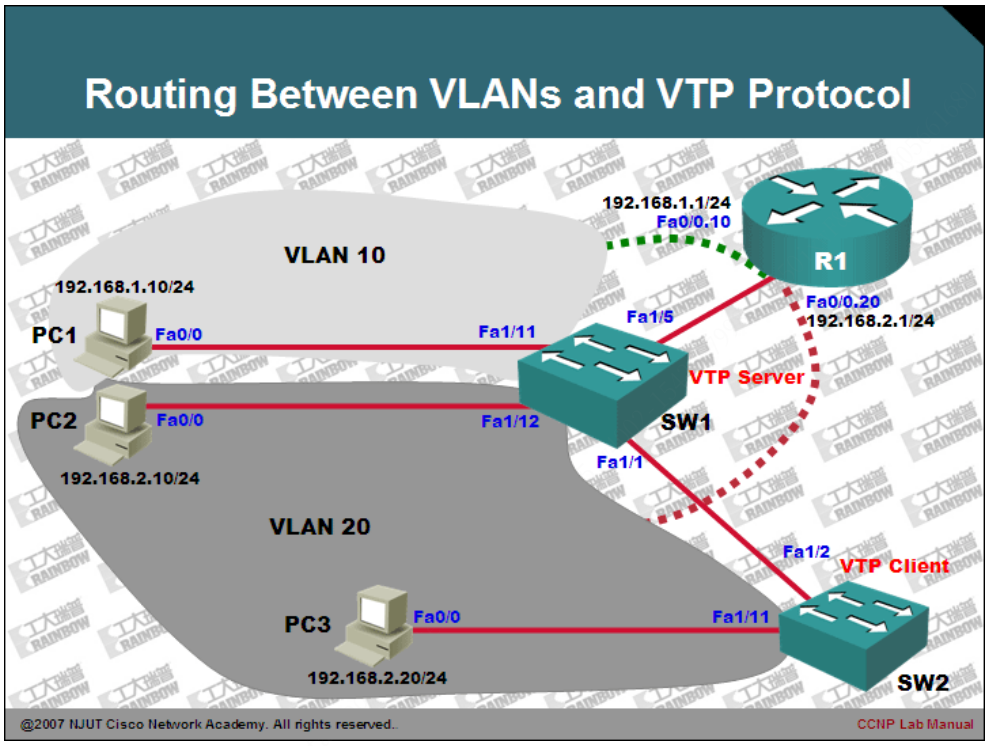
Lab 54. Routing Between VLANs and VTP Protocol

实验目的：

1、掌握 VTP 配置方法。

2、掌握 VLAN 间路由配置方法以及子接口的配置。

实验拓扑图：



实验步骤及要求：

1、配置 PC1、PC2 和 PC3 用于模拟主机，配置如下：

```
PC1(config)#no ip routing
PC1(config)#
PC1(config)#ip default-network 192.168.1.1
PC1(config)#
PC1(config)#interface fastEthernet 0/0
PC1(config-if)#ip address 192.168.1.10 255.255.255.0
PC1(config-if)#no shutdown
PC1(config-if)#exit
PC1(config)#
```

批注 [stanley519]：关闭路由功能。

批注 [stanley520]：配置 PC1 的默认网关为 192.168.1.1。

```
PC2(config)#no ip routing
PC2(config)#
PC2(config)#ip default-network 192.168.2.1
PC2(config)#
PC2(config)#interface fastEthernet 0/0
PC2(config-if)#ip address 192.168.2.10 255.255.255.0
PC2(config-if)#no shutdown
PC2(config-if)#exit
PC2(config)#
```

```
PC3(config)#no ip routing
PC3(config)#
PC3(config)#ip default-network 192.168.2.1
PC3(config)#
PC3(config)#interface fastEthernet 0/0
PC3(config-if)#ip address 192.168.2.20 255.255.255.0
PC3(config-if)#no shutdown
PC3(config-if)#exit
PC3(config-if)#
```

2、首先配置 SW1 与 SW2 的 TRUNK，配置如下：

```
SW1(config)#interface fastEthernet 1/1
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

批注 [stanley521]：选择 TRUNK 的封闭协议。

批注 [stanley522]：指定接口为 TRUNK 模式。

```
SW2(config)#interface fastEthernet 1/2
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
```

批注 [stanley523]：指定与 SW1 相同的 TRUNK 封闭协议。

```
SW2(config-if)#exit
```

3、查看 TRUNK 信息：

```
SW2#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa1/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa1/2       1-1005

Port        Vlans allowed and active in management domain
Fa1/2       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa1/2       1
SW2#
```

批注 [stanley524]：当时 Fa1/2 的接口处于 TRUNK 状态。并且其使用 DOT1Q 的 TRUNK 协议。同时，其 Native Vlan 为 1.

批注 [stanley525]：允许在 TRUNK 的传输数据的 VLAN 列表。

4、在配置 VTP 协议之前，先查看 SW1 或 SW2 的 VTP 的状态：

```
SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 256
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

批注 [stanley526]：VTP 的协议版本号。VTP 的版本 2，增加了对令牌环网的支持。

批注 [stanley527]：VTP 的配置版本号，指出了 VLAN 的变更信息。

批注 [stanley528]：默认情况下，所有交换机都为 VTP 的 Server 模式。

批注 [stanley529]：VTP 的修剪。

批注 [stanley530]：VTP 的密码。

5、配置 SW1 与 SW2 的 VTP 协议：

```
SW1#vlan database
SW1(vlan)#vtp domain ccnp
Changing VTP domain name from NULL to ccnp
SW1(vlan)#
SW1(vlan)#vtp server
Device mode already VTP SERVER.
SW1(vlan)#
SW1(vlan)#vtp password cisco
Setting device VLAN database password to cisco.
SW1(vlan)#
SW1(vlan)#vtp pruning
```

批注 [stanley531]：配置 VTP 的域名为 ccnp。

批注 [stanley532]：配置前交换机为 server 模式。

批注 [stanley533]：为了确保 VTP 的安全，可以在此处配置密码。

批注 [stanley534]：启用 VTP 的修剪功能。VTP 修剪功能能够有效的减少不必要的泛洪，从而增加有效的可用带宽。

```
SW1(vlan)#
```

也可以从全局配置模式，配置 VTP 协议：

```
SW2(config)#vtp password cisco
Setting device VLAN database password to cisco
SW2(config)#
SW2(config)#vtp domain ccnp
Changing VTP domain name from fuckcisco to ccnp
SW2(config)#
SW2(config)#vtp pruning
Pruning switched on
SW2(config)#
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2(config)#
```

批注 [stanley535]：VTP 的密码。

批注 [stanley536]：指定 VTP 的域。

批注 [stanley537]：开启 VTP 的修剪功能。

批注 [stanley538]：指定当前交换机的 VTP 的工作模式。

6、查看 SW1 或是 SW2 的 VTP 的状态信息：

```
SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : ccnp
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x71 0x62 0x0B 0xD1 0xED 0xFD 0x7D 0xAC
Configuration last modified by 199.1.1.3 at 3-2-93 02:11:08
SW2#
```

7、在 SW1 和 SW2 上创建 VLAN：

```
SW1#vlan database
SW1(vlan)#vlan 10 name cisco
VLAN 10 added:
    Name: cisco
SW1(vlan)#exit
APPLY completed.
Exiting....
SW1#
SW1#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
SW1(config)#
SW1(config)#vlan 20
SW1(config-vlan)#name microsoft
```

批注 [stanley539]：进入到 VLAN DATABASE 配置模式。

批注 [stanley540]：创建一个 VLAN 其编号为 10，同时指定其名称为 cisco。

批注 [stanley541]：在全局配置模式下，创建一个编号为 20 的 VLAN。

批注 [stanley542]：指定新建的 VLAN 的名称为 microsoft。

```
SW1(config-vlan)#exit
```

8、查看 SW1 的 VLAN 配置：

```
SW1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/2, Fa1/3, Fa1/4
                                                Fa1/5, Fa1/6, Fa1/7, Fa1/8
                                                Fa1/9, Fa1/10, Fa1/11, Fa1/12
                                                Fa1/13, Fa1/14, Fa1/15
10   cisco                            active
20   microsoft                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
SW1#
```

批注 [stanley543]：自定义的 VLAN。

9、查看 VTP 的状态信息：

```
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 256
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : ccnp
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xF3 0x1C 0x33 0x46 0xEA 0x14 0xBB 0x9F
Configuration last modified by 0.0.0.0 at 3-1-02 00:52:53
Local updater ID is 0.0.0.0 (no valid interface found)
SW1#
```

批注 [stanley544]：由于对创建了两个 VLAN，导致 VTP 的配置版本号变为 2。

10、查看 SW2 的 VTP 的状态信息：

```
SW2#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 256
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : ccnp
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xF3 0x1C 0x33 0x46 0xEA 0x14 0xBB 0x9F
Configuration last modified by 0.0.0.0 at 3-1-02 00:52:53
SW2#
```

批注 [stanley545]：SW2 的交换机 VTP 的配置版本，此时为 2。

11、查看 SW2 的 VLAN 信息：

```
SW1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   cisco                            active
20   microsoft                        active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
.....
```

批注 [stanley546]：从 SW2 通过 VTP 的协议，成功的同步了 SERVER 角色的交换机 SW1 的 VLAN 配置信息。

12、在 SW1 和 SW2 上将相应 VLAN 的主机端口加入到 VLAN：

```
SW1(config)#interface fastEthernet 1/11
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
SW1(config)#
SW1(config)#interface fastEthernet 1/12
SW1(config-if)#switchport access vlan 20
SW1(config-if)#exit
```

批注 [stanley547]：将当前接口加入到 VLAN 10。

在 SW2 上配置 VLAN：

```
SW2(config)#interface fastEthernet 1/11
SW2(config-if)#switchport access vlan 20
SW2(config-if)#exit
```

13、在 PC1 和 PC2 及 PC3 上使用 ping 命令测试 VLAN 间的通信：

```
PC1#ping 192.168.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC1#
```

批注 [stanley548]：在 PC1 上向 VLAN 2 的主机发送 ICMP 的数据包，结果无法 PING 通。

```
PC2#ping 192.168.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 24/24/24 ms
PC2#
PC2#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC2#
```

批注 [stanley549]：相同 VLAN 之间是可以通信的。

批注 [stanley550]：不同的 VLAN 是不可以相互通信的。

```
PC3#ping 192.168.2.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/18/32 ms
PC3#
PC3#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC3#
```

14、在 R1 上配置单臂路由，确保两个 VLAN 之间通信。

15、首先配置 R1 与 SW1 之间的 TRUNK 链路，配置如下：

```
SW1(config)#interface fastEthernet 1/5
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

```
R1(config)#
R1(config)#interface fastEthernet 0/0
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
```

批注 [stanley551]：配置子接口，需要将物理接口 IP 删除掉，同时激活物理接口。

批注 [stanley552]：启用 FA0/0.10 子接口。

批注 [stanley553]：此命令主要的目的是接收 VLAN 10 的数据包，同时发出的数据包会被打上 10 的 VLAN 的标记。

批注 [stanley554]：配置 IP 用于 VLAN 10 的默认网关。

16、查看 R1 的路由表：

```
R1#show ip route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0.10
C    192.168.2.0/24 is directly connected, FastEthernet0/0.20
R1#
```

批注 [stanley555]：子接口直连路由。

17、在 PC1、PC2 和 PC3 使用 ping 命令测试 VLAN 间路由：

```
PC1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/232/1040 ms
PC1#
PC1#ping 192.168.2.1
```

批注 [stanley556]：此时可以 ping 通默认网关。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/223/1012 ms
PC1#
PC1#ping 192.168.2.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 12/48/92 ms
PC1#
PC1#ping 192.168.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 20/52/96 ms
PC1#
```

批注 [stanley557]：可以 ping 通 vlan 20 的默认网关。

批注 [stanley558]：可以 ping 通 vlan 20 的 pc2 主机。

```
PC2#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/48/88 ms
PC2#
```

批注 [stanley559]：此时 PC2 也可以通过 VLAN 间路由 PING 通 PC1 的主机。

```
PC3#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/50/88 ms
PC3#
```

批注 [stanley560]：位于 VLAN 20 的 PC3 也可以 PING 通 VLAN 10 的 PC1 主机。

18、实验完成。

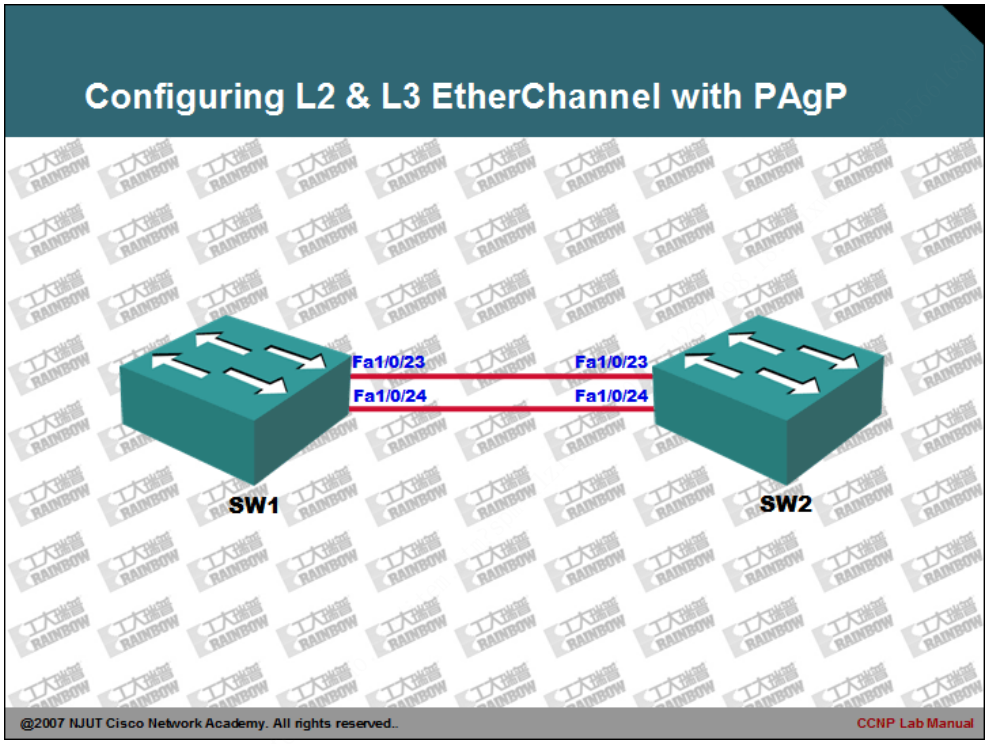
CCNP Lab Manual

Lab 55. Configuring L2 & L3 EtherChannel with PAgP

实验目的：

1、掌握其于 Cisco 私有的 PAgP 的链路聚合协议的配置方法。
2、掌握第二层与第三层的 PAgP 配置区别。
3、PAgP 为 Cisco 私有链路聚合协议。

实验拓扑图：



实验步骤及要求：

1、本实验使用两台 Cisco Catalyst 3750 交换机。并按照拓扑连接相应的交换机的线缆。

2、为了能够保证实验成功，因此建议将 Fa1/0/1 - 22 号接口置为 shutdown 状态。

3、在 SW1 或 SW2 上查看交换机的 STP 信息：

```
SW1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0014.a8e2.9880
             Cost        19
             Port        25 (FastEthernet1/0/23)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0014.a8f1.9880
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa1/0/23         Root FWD 19        128.25   P2p
Fa1/0/24         Altn BLK 19        128.26   P2p

SW1#
```

批注 [stanley561]：默认情况下，交换机会使用 STP 协议阻塞其中的某个端口。因为交换机认为网络有环路存在。

4、STP 协议虽然可以避免网络环路的问题。但是其仍然不能充分的利用冗余的链路带宽。为了解决链路带宽的问题，可以实施 PAgP 的链路聚合。

5、在 SW1 和 SW2 上配置如下：

```
SW1(config)#interface range fastEthernet 1/0/23 - 24
SW1(config-if-range)#switchport
SW1(config-if-range)#channel-protocol pagp
SW1(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

SW1(config-if-range)#exit
SW1(config)#exit
```

批注 [stanley562]：进入 23，24 号端口。

批注 [stanley563]：开启交换机的二层特性。此条命令默认是被启用的。

批注 [stanley564]：指定聚合的协议。

批注 [stanley565]：将当前端口组加入到 channel-group 即聚合链路通道 1。同时将聚合工作模式设置为积极模式。

```
SW2(config)#interface range fastEthernet 1/0/23 - 24
SW2(config-if-range)#sw
SW2(config-if-range)#switchport
SW1(config-if-range)#channel-protocol pagp
SW2(config-if-range)#channel-group 1 mode auto
Creating a port-channel interface Port-channel 1

SW2(config-if-range)#exit
SW2(config)#exit
```

批注 [stanley566]：指定聚合的协议。

批注 [stanley567]：将端口组加入到聚合链路通道 1。同时将其设置为自动模式。

6、处于 PAgP 的 Descirable 模式的接口，其会主动的进入协商状态。而 Auto 模式会进入被动的进入协商状态。

7、当在两台交换机完成相应配置后，IOS 在配置过程中，会给出如下提示信息：

```
00:32:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/23, changed state
to down
00:32:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/24, changed state
to down

00:32:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/23, changed state
to up
00:32:38: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/24, changed state
to up

0:37:18: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:37:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

批注 [stanley568]：当改变接口工作方式后，会导致接口的 DOWN。

批注 [stanley569]：交换机在重置端口将其置为 UP 状态。

批注 [stanley570]：当与对端交换机协商成功后，其 port-channel 1 的会进入 UP 状态。指出链路聚合配置成功。

8、查看 SW1 的接口的聚合信息：

```
SW1#show interfaces fastEthernet 1/0/23 etherchannel
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Desirable-Sl     Gcchange = 0
Port-channel  = Po1         GC   = 0x00010001      Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers Interval Count   Priority   Method   Ifindex
Fa1/0/23    SC    U6/S7   H      30s      1         128        Any      5001
```

批注 [stanley571]：聚合组及其工作模式。

批注 [stanley572]：聚合使用协议。

批注 [stanley573]：本地被聚合的接口信息。

```
Partner's information:

          Partner                 Partner          Partner         Partner Group
Port      Name                    Device ID        Port       Age  Flags   Cap.
Fa1/0/23  SW2                     0014.a8e2.9880   Fa1/0/23    20s SAC     10001

Age of the port in the current state: 00d:00h:06m:53s


SW1#
```

批注 [stanley574]: 对端的聚合的接口信息。

9、使用 show etherchannel port-channel 命令查看聚合组信息：

```
SW1#show etherchannel port-channel
                Channel-group listing:
                ----------------------


Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1
------------

Age of the Port-channel   = 00d:00h:15m:37s
Logical slot/port   = 10/1          Number of ports = 2
GC                  = 0x00010001      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   PAgP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa1/0/23 Desirable-Sl       0
  0     00     Fa1/0/24 Desirable-Sl       0

Time since last port bundled:    00d:00h:10m:27s    Fa1/0/24


SW1#
```

批注 [stanley575]: 处于聚合组的一些端口列表。

10、查看聚合链路的汇总信息：

```
SW1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa1/0/23(P) Fa1/0/24(P)

SW1#
```

批注 [stanley576]: 关键字（SU）中的 S 指出当前的聚合路链路属于第二层聚合。

11、查看生成树信息：

```
SW1#show spanning-tree

.........

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Root FWD 12        128.616  P2p

SW1#
```

批注 [stanley577]: 此时，生成树协议仅针对被聚合的逻辑端口工作。

12、配置 SW1 和 SW2 的 VLAN 1 的 IP 地址，测试聚合链路的容错：

```
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
```

```
SW2(config)#interface vlan 1
SW2(config-if)#ip address 192.168.1.2 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#exit
```

13、在 R1 上使用 ping 命令，测试两台交换机的连接：

```
SW2#ping 192.168.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SW2#
```

14、为了能够测试聚合端口的冗余容错特性，在 SW2 上使用扩展的 ping 命令向 SW1 持续发送 ICMP 数据包：

```
SW2#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]: 1000000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1000000, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

批注 [stanley578]：配置目标地址。

批注 [stanley579]：将 PING 的值设置一个较大的值。

15、然后在 SW1 上将聚合组中的 Fastethernet 1/0/24 或 Fastethernet 1/0/24 任一端口手工 shutdown 后，观察 SW2 的 ping 的反馈信息。会发现其 Ping 数据包不会出现中断，说明**链路聚合能够有效的避免单链路的拓扑不稳定，同时解决了冗余链路情况下，由于生成树原因而不能充分利用链路带宽和实现负载分担的问题。**

16、之前所配置的是第二层的 PAgP 的链路聚合，接下来配置向各位展示了如何配置第三层的 PAgP 的链路聚合。

17、首先删除之前的二层 PAgP 的配置。

18、在 SW1 和 SW2 上作如下配置：

```
SW1(config)#interface port-channel 1
SW1(config-if)#no switchport
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#
SW1(config)#
SW1(config)#interface range fastEthernet 1/0/23 - 24
SW1(config-if-range)#no switchport
SW1(config-if-range)#channel-protocol pagp
```

批注 [stanley580]：关闭交换机接口的二层特性。

```
SW1(config-if-range)#channel-group 1 mode desirable
SW1(config-if-range)#exit
SW1(config)#exit
SW1#
00:12:15: %EC-5-L3DONTBNDL1: Fa1/0/23 suspended: PAgP not enabled on the remote port.
00:12:16: %EC-5-L3DONTBNDL1: Fa1/0/24 suspended: PAgP not enabled on the remote port.
```

批注 [stanley581]：由于目前仅配置 SW1，而 SW2 并没有配置。所以此处系统提示，远程主机没有激活 PAgP 聚合。

```
SW2(config)#interface port-channel 1
SW2(config-if)#no switchport
SW2(config-if)#ip address 192.168.1.2 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#exit
SW2(config)#
SW2(config)#interface range fastEthernet 1/0/23 - 24
SW2(config-if-range)#no switchport
SW2(config-if-range)#channel-protocol pagp
SW2(config-if-range)#channel-group 1 mode desirable
SW2(config)#exit
SW2#
00:20:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/23, changed state
to up
00:20:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/24, changed state
to up
00:20:03: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:20:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
```

批注 [stanley582]：当配置完 SW2 交换机后，系统提示聚合链路已经处于 UP 状态。

17、查看聚合链路的信息：

```
SW2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
```

```
1       Po1(RU)          PAgP       Fa1/0/23(P) Fa1/0/24(P)

SW2#
```

批注 [stanley583]：RU 的状态的其中，R 指出目前聚合链路为第三层的聚合。

18、使用 Ping 命令检测：

```
SW2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
SW2#
```

19、使用步骤 14 和步骤 15 检查第三层的聚合链路的容错性。具体不再列出。

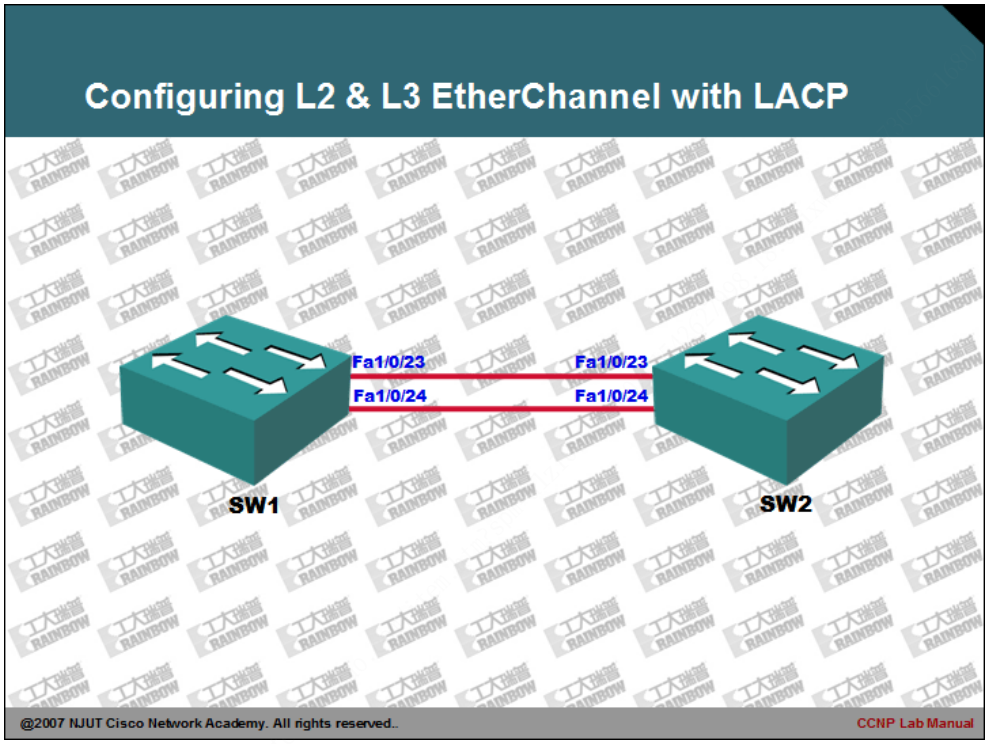
20、实验完成。

Lab 56. Configuring L2 & L3 EtherChannel with LACP

实验目的：

1、掌握其于 Cisco 私有的 LACP 的链路聚合协议的配置方法。
2、掌握第二层与第三层的 LACP 配置区别。
3、LACP 为公开标准链路聚合协议。

实验拓扑图：



实验步骤及要求：

1、本实验使用两台 Cisco Catalyst 3750 交换机。并按照拓扑连接相应的交换机的线缆。

2、为了能够保证实验成功，因此建议将 Fa1/0/1 - 22 号接口置为 shutdown 状态。

3、由于 LACP 的工作特性与 PAgP 非常相似，因此本次实验仅列出 LACP 的配置命令，具体解释请参看**实验：Configuring L2 & L3 EtherChannel with LAC** 一节。

4、首先在 SW1 和 SW2 交换机上配置第二层的 LACP 的链路聚合：

```
SW1(config)#interface range fastEthernet 1/0/23 - 24
SW1(config-if-range)#channel-protocol lacp
SW1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

SW1(config-if-range)#exit
```

```
SW2(config)#interface range fastEthernet 1/0/23 - 24
SW2(config-if-range)#channel-protocol lacp
SW2(config-if-range)#channel-group 1 mode passive
SW2(config-if-range)#exit
```

5、查看 SW1 或 SW2 的 LACP 汇总信息：

```
SW1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)         LACP      Fa1/0/23(P) Fa1/0/24(P)
SW1#
```

批注 [stanley584]：第二层的 LACP 聚合。

5、在两台交换机配置 VLAN 1 的 IP 地址，用于测试，并且建议各位使用扩展的

ping 命令去测试聚合链路的容错：

```
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#
```

```
SW2(config)#interface vlan 1
SW2(config-if)#ip address 192.168.1.2 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#exit
```

Ping 的命令信息如下：

```
SW1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
SW1#
```

6、删除之前的第二层的 LACP 的配置或重启交换机。

7、在两台交换机配置第三层的 LACP 的链路聚合：

```
SW1(config)#interface port-channel 1
SW1(config-if)#no switchport
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#
SW1(config)#interface range fastEthernet 1/0/23 - 24
SW1(config-if-range)#no switchport
SW1(config-if-range)#channel-protocol lacp
SW1(config-if-range)#channel-group 1 mode active
SW1(config-if-range)#exit
```

```
SW2(config)#interface port-channel 1
SW2(config-if)#no switchport
SW2(config-if)#ip address 192.168.1.2 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#exit
SW2(config)#
SW2(config)#interface range fastEthernet 1/0/23 - 24
```

```
SW2(config-if-range)#no switchport
SW2(config-if-range)#channel-protocol lacp
SW2(config-if-range)#
SW2(config-if-range)#channel-group 1 mode passive
SW2(config-if-range)#exit
SW2(config)#exit
```

8、查看聚合链路的汇总信息：

```
SW2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(RU)         LACP      Fa1/0/23(P) Fa1/0/24(P)

SW2#
```

批注 [stanley585]：R 关键字指示出当前聚合为三层链路聚合。

```
SW1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
```

```
------+-------------+-----------+--------------------------------------------
1       Po1(RU)          LACP      Fa1/0/23(P) Fa1/0/24(P)


SW1#
```

9、使用 ping 命令测试：

```
SW2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
SW2#
```

10、实验完成。

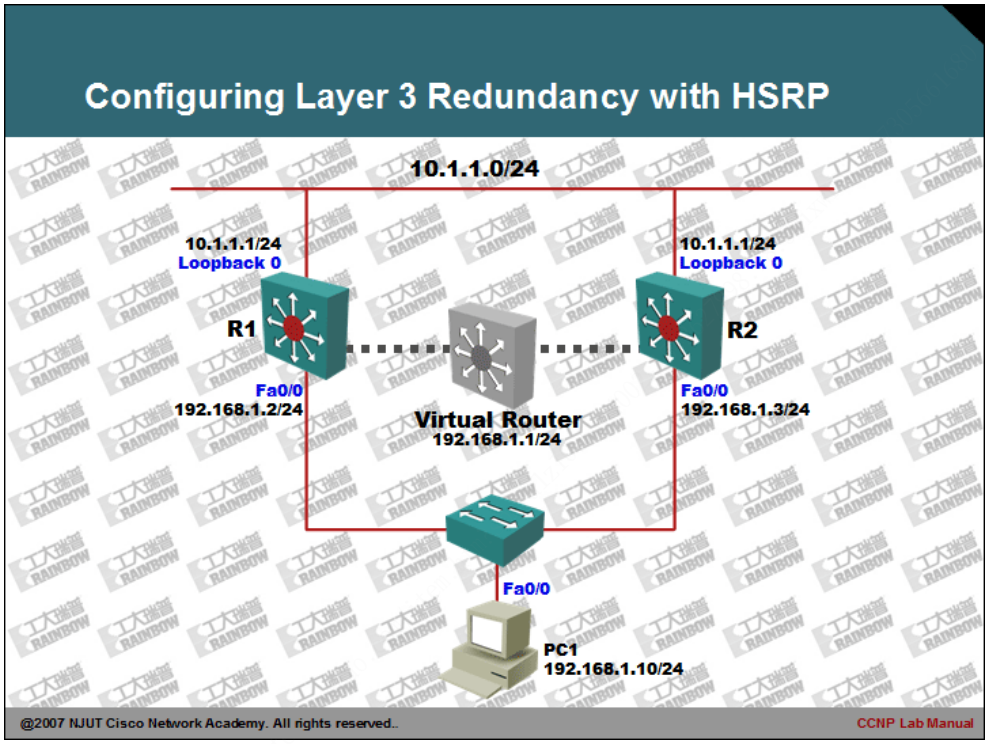
CCNP Lab Manual

Lab 57. Configuring Layer 3 Redundancy with HSRP

实验目的：

1、理解 HSRP 的工作原理。
2、掌握 HSRP 配置方法.
3、理解 HSRP 的抢占与跟踪作用。

实验拓扑图：



实验步骤及要求：

1、本实验可以使用三层交换机完成,也可以使用路由器完成,在使用路由器时需要注意 IOS 的版本,确认支持 HSRP 协议。

2、配置 R1 与 R2 路由器的接口 IP 地址：

```
R1(config)#interface loopback 0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.2 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

```
R2(config)#interface loopback 0
R2(config-if)#ip address 10.1.1.1 255.255.255.0
R2(config-if)#exit
R2(config)#
R2(config)#interface fastEthernet 0/0
R2(config-if)#ip address 192.168.1.3 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

注意：在 R1 与 R2 上配置的环回口地址均为 10.1.1.1/24 主要是用于模拟某主机与 R1 和 R2 直连。

3、配置路由器 PC1 将与模拟成客户端，为了确保网关的冗余，因此将 PC1 的网关指向，即将通过 HSRP 协议虚拟出的虚拟网关地址：

```
PC1(config)#no ip routing
PC1(config)#
PC1(config)#interface fastEthernet 0/0
PC1(config-if)#ip address 192.168.1.10 255.255.255.0
PC1(config-if)#no shutdown
PC1(config-if)#exit
PC1(config)#
PC1(config)#ip default-gateway 192.168.1.1
PC1(config)#exit
PC1#
```

4、在 PC1 上使用 ping 命令测试当前是否可以到达 10.1.1.1/24 的主机：

```
PC1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC1#
```

批注 [stanley586]：由于目前 192.168.1.1 网关并不存在，因此此时无法 ping 通目标主机。

4、为了能够有效的确保网关的冗余，因此在 R1 与 R2 上配置 HSRP 协议，配置如下：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#standby 1 ip 192.168.1.1
```

批注 [stanley587]：启用 HSRP 组 1，并且设置组 1 的虚拟 IP 地址为 192.168.1.1

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#standby 1 ip 192.168.1.1
```

5、当在 R1 上配置 HSRP 组后，IOS 会提示如下信息：

```
00:13:27: %STANDBY-6-STATECHANGE: FastEthernet0/0 Group 1 state Standby -> Active
```

批注 [stanley588]：指出当前 R1 为 ACTIVE 路由器，负责 ARP 响应和三层路由任务。

6、在 R1 或 R2 上查看 HSRP 组信息：

```
R1#show standby
FastEthernet0/0 - Group 1
  Local state is Active, priority 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 1.348
  Virtual IP address is 192.168.1.1 configured
  Active router is local
  Standby router is 192.168.1.3, priority 100 expires in 7.812
  Virtual mac address is 0000.0c07.ac01
  5 state changes, last state change 00:00:10
  IP redundancy name is "hsrp-Fa0/0-1" (default)
R1#
```

批注 [stanley589]：R1 当前的脚色为 ACTIVE 路由器。其优先级为 100。
HSRP 的 Hello 数据包的发送周期和其保持时间。
HSRP 的 Hello 数据包能够用于监测 ACTIVE 路由器的状态。

批注 [stanley590]：虚拟路由器的 IP 地址。

批注 [stanley591]：虚拟路由器的 MAC 地址。

```
R2#show standby
FastEthernet0/0 - Group 1
  Local state is Standby, priority 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.686
  Virtual IP address is 192.168.1.1 configured
  Active router is 192.168.1.2, priority 100 expires in 7.748
  Standby router is local
  8 state changes, last state change 00:03:11
  IP redundancy name is "hsrp-Fa0/0-1" (default)
```

```
R2#
```

7、HSRP 组中的每台路由器均会带有一个优先级。优先级会影响哪一台路由器成为 ACTIVE 路由器，用于响应客户端的 ARP 请求。如果在 HSRP 刚启动，而且每台路由器的优先级均相同，则会优先选择接口 IP 较高的为 ACTIVE 路由器。

8、在 PC1 客户端，使用 ping 和 traceroute 命令跟踪路由：

```
PC1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/300/1100 ms
PC1#
PC1#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

  1 192.168.1.2 68 msec 56 msec *
PC1#
```

批注 [stanley592]：由于当前 R1 为 ACTIVE 路由器，因此此时显示的下一跳为 192.168.1.2，即 R1 路由器。

9、查看 PC1 的客户端的 ARP 缓存：

```
PC1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.10           -   ca02.0be4.0000  ARPA   FastEthernet0/0
Internet  192.168.1.1           12   0000.0c07.ac01  ARPA   FastEthernet0/0
PC1#
```

批注 [stanley593]：当前虚拟网关的 IP 地址。

其中 MAC 地址含义：
0000.0c 为 Cisco 厂商标识
0c.ac 为 HSRP 组标识
01 为 HSRP 组号

10、使用扩展 ping 命令向 10.1.1.1 发送较多数据包，同时将 R1 的 Fa0/0 接口，手工置为 down 状态，观察 HSRP 的冗余：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#shutdown
00:39:48: %STANDBY-6-STATECHANGE: FastEthernet0/0 Group 1 state Active -> Init
```

批注 [stanley594]：当将 R1 路由器置为 DOWN 状态后，其 HSRP 组会立即进入到 Init 状态。并且丢失 Active 状态。

查看 PC1 上的扩展 ping:

```
PC1#ping
Protocol [ip]:
Target IP address: 10.1.1.1
Repeat count [5]: 1000000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
```

批注 [stanley595]：发送较多的数据包。

```
Type escape sequence to abort.
Sending 1000000, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.....!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (456/461), round-trip min/avg/max = 16/72/560 ms
PC1#
```

从上面信息可以看出，由于R1的Fa0/0接口故障，导致PC1无法到达10.1.1.0/24的网络。另外，由于R1的Fa0/0接口故障，R2将无法收到Active路由器发送的Hello数据包，因此，在R2默认的HSRP的保持时间10秒超时后，R2会立即将自己提升为Active路由器，通过如下的信息可以确认该结论：

```
00:39:56: %STANDBY-6-STATECHANGE: FastEthernet0/0 Group 1 state Standby -> Active
```

11、此时，再次在PC1上使用ping和traceroute命令确认路由和目标主机可达：

```
PC1>ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/57/108 ms
PC1>
PC1>traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

  1 192.168.1.3 32 msec 28 msec *
PC1>
```

批注 [stanley596]：此时下一跳为R2路由器。

12、通过以上上步骤，HSRP可以有效的保障网关的冗余，确保网络稳定。

13、将R1路由器的Fa0/0接口置为UP状态：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

14、在等待一段时间后，再次在R1或R2路由器查看HSRP组信息：

```
R1#show standby
FastEthernet0/0 - Group 1
  Local state is Standby, priority 100
  Hellotime 3 sec, holdtime 10 sec
```

批注 [stanley597]：R1路由器保持Standby状态。

```
  Next hello sent in 0.450
  Virtual IP address is 192.168.1.1 configured
  Active router is 192.168.1.3, priority 100 expires in 9.672
  Standby router is local
  7 state changes, last state change 00:00:34
  IP redundancy name is "hsrp-Fa0/0-1" (default)
R1#
```

批注 [stanley598]：指出 Active 路由器的信息。

15、如果 R1 路由器为一台性能较好的路由器，而 R2 仅仅为备份路由器，因此可能更希望当 R1 路由器恢复时，能够负责 ARP 的响应和三层路由任务。为了实现这一功能，需要为 R1 路由器配置较高的优先级和开启 HSRP 的抢占功能：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#standby 1 priority 200
R1(config-if)#standby 1 preempt
R1(config-if)#exit
R1(config)#
```

批注 [stanley599]：设置 R1 路由器的 HSRP 的优先级为:200。

批注 [stanley600]：启用抢占。

16、此时会注意到 R1 路由器系统会给出如下提示信息：

```
R1#
00:55:55: %STANDBY-6-STATECHANGE: FastEthernet0/0 Group 1 state Standby -> Active
R1#
```

批注 [stanley601]：R1 路由器立即获得 Acitve 状态。

17、在 R2 上查看 HSRP 组信息：

```
R2#show standby
FastEthernet0/0 - Group 1
  Local state is Standby, priority 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.722
  Virtual IP address is 192.168.1.1 configured
  Active router is 192.168.1.2, priority 200 expires in 7.452
  Standby router is local
  11 state changes, last state change 00:03:53
  IP redundancy name is "hsrp-Fa0/0-1" (default)
R2#
```

批注 [stanley602]：当前路由器的优先级。

批注 [stanley603]：Acitve 路由器优先级。

18、**HSRP 除了能够对下行链路实施冗余，同时还可以对上行链路进行监测**，动态的变更 Active 角色，确保网络万无一失。下面给出如何配置 HSRP 的接口跟踪功能：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#standby 1 priority 200
R1(config-if)#standby 1 preempt
R1(config-if)#standby 1 track loopback 0 150
R1(config-if)#exit
```

批注 [stanley604]：配置 HSRP 对其上行链路实施跟踪，如果被跟踪的链路出现故障，立即将当前优先级降低 150，以便于其它路由器可以抢占 Acitve，保证网络稳定。

```
R1(config)#
```

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#standby 1 preempt
R2(config-if)#
```

批注 [stanley605]: R2 需要开启抢占。

19、在 R1 上将其 loopback 0 接口，手工置为 down 状态，然后观察系统提示信息：

```
R1#debug standby events
HSRP Events debugging is on
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#interface loopback 0
R1(config-if)#shutdown
R1(config-if)#
R1(config-if)#
01:09:58: SB: Fa0/0 Grp 1 Tracked interface Loopback0 Down
01:09:58: SB: Fa0/0 Grp 1 Priority 200/200 -> 50/200
01:09:58: SB1: Fa0/0 Active: j/Coup rcvd from higher pri router (100/192.168.1.3)
01:09:58: SB1: Fa0/0 Active router is 192.168.1.3, was local
01:09:58: SB:  Fa0/0 Remove active hash 192.168.1.2 (vIP 192.168.1.1)
01:09:58: SB:  Fa0/0 Remove passive hash 192.168.1.3 (frc 0)
01:09:58: SB:  Fa0/0 Add active hash 192.168.1.3 (vIP 192.168.1.1)
01:09:58: SB1: Fa0/0 Standby router is unknown, was 192.168.1.3
01:09:58: SB1: Fa0/0 Active -> Speak
01:09:58: %STANDBY-6-STATECHANGE: FastEthernet0/0 Group 1 state Active -> Speak
01:09:58: SB1: Fa0/0 Redundancy "hsrp-Fa0/0-1" state Active -> Speak
01:09:58: SB:  Fa0/0 Redirect adv start
01:09:58: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
01:10:08: SB1: Fa0/0 Speak: d/Standby timer expired (unknown)
01:10:08: SB1: Fa0/0 Standby router is local
01:10:08: SB1: Fa0/0 Speak -> Standby
01:10:08: SB1: Fa0/0 Redundancy "hsrp-Fa0/0-1" state Speak -> Standby
```

批注 [stanley606]: 启用对 HSRP 的调试。

批注 [stanley607]: HSRP 组跟踪到上链路出现故障。

批注 [stanley608]: 将当前的优先级降低 150。

批注 [stanley609]: R1 路由器进入 Speack 状态。

20、查看 R1 与 R2 路由器 HSRP 组信息：

```
R1#show standby
FastEthernet0/0 - Group 1
  Local state is Standby, priority 50 (confgd 200), may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.668
  Virtual IP address is 192.168.1.1 configured
```

```
  Active router is 192.168.1.3, priority 100 expires in 8.252
  Standby router is local
  13 state changes, last state change 00:01:19
  IP redundancy name is "hsrp-Fa0/0-1" (default)
  Priority tracking 1 interface, 0 up:
    Interface                 Decrement  State
    Loopback0                   150      Down  (administratively down)
R1#
```

```
R2#show standby
FastEthernet0/0 - Group 1
  Local state is Active, priority 100, may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.808
  Virtual IP address is 192.168.1.1 configured
  Active router is local
  Standby router is 192.168.1.2, priority 50 expires in 9.128
  Virtual mac address is 0000.0c07.ac01
  15 state changes, last state change 00:00:57
  IP redundancy name is "hsrp-Fa0/0-1" (default)
  Priority tracking 1 interface, 1 up:
    Interface                 Decrement  State
    Loopback0                   10       Up
```

21、实验完成。

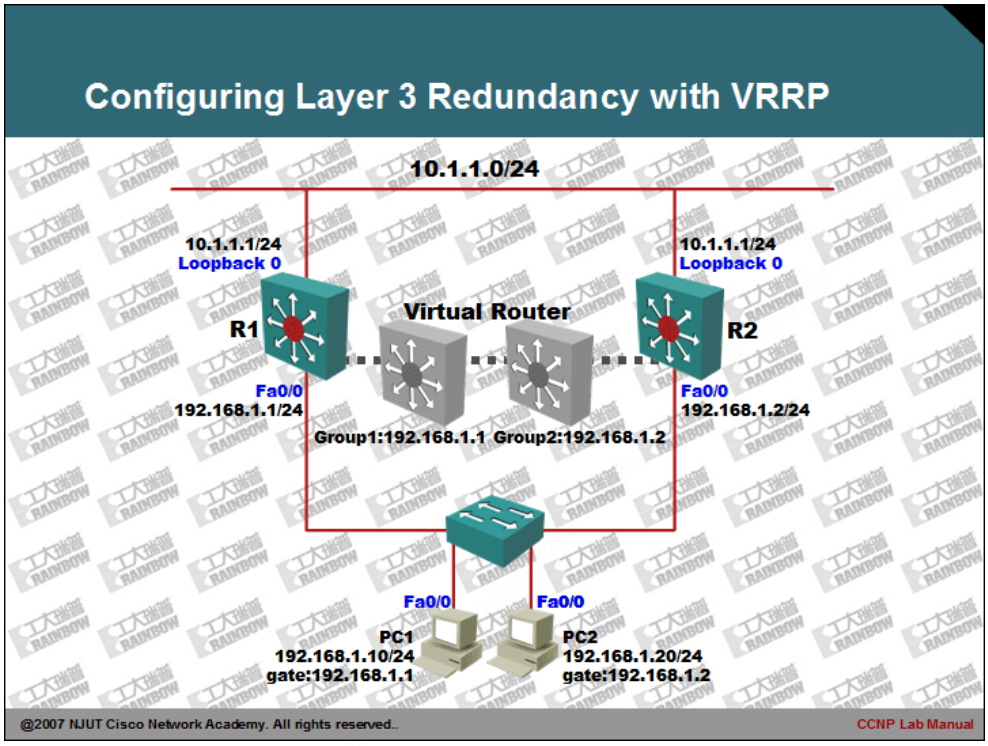
CCNP Lab Manual

Lab 58. Configuring Layer 3 Redundancy with VRRP

实验目的：

1、掌握第三层网关冗余协议的 VRRP 配置。

实验拓扑图：



实验步骤及要求：

1、本实验可以使用三层交换机完成,也可以使用路由器完成,在使用路由器时需要注意 IOS 的版本,确认支持 HSRP 协议。

2、配置 PC1 与 PC2 路由器，将其模拟成主机，配置如下：

```
PC1(config)#no ip routing
PC1(config)#
PC1(config)#interface fastEthernet 0/0
PC1(config-if)#ip address 192.168.1.10 255.255.255.0
PC1(config-if)#no cdp enable
PC1(config-if)#no shutdown
PC1(config-if)#exit
PC1(config)#
PC1(config)#ip default-gateway 192.168.1.1
PC1(config)#exit
PC1#
```

批注 [stanley610]: PC1 的默认网关指向 192.168.1.1。

```
PC2(config)#no ip routing
PC2(config)#
PC2(config)#interface fastEthernet 0/0
PC2(config-if)#ip address 192.168.1.20 255.255.255.0
PC2(config-if)#no cdp enable
PC2(config-if)#no shutdown
PC2(config-if)#exit
PC2(config)#
PC2(config)#ip default-gateway 192.168.1.2
PC2(config)#exit
PC2#
```

批注 [stanley611]: PC2 的默认网关指向 192.168.1.2。

3、首先在 PC1 和 PC2 上使用 ping 和 traceroute 命令，确认网络是否可达：

```
PC1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/60/72 ms
PC1#
PC1#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1
```

```
 1 192.168.1.1 12 msec *  96 msec
PC1#
```

批注 [stanley612]：PC1 到达目标网络，其下一跳为 192.168.1.1。

```
PC2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/293/1084 ms
PC2#
PC2#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1 192.168.1.2 120 msec *  72 msec
PC2#
```

批注 [stanley613]：PC2 到达目标网络，其下一跳为 192.168.1.2。

4、将 R1 路由器的 FA0/0 接口，置为 down 状态：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#shutdown
R1(config-if)#
```

5、再次在 R1 和 R2 上使用 ping 和 traceroute 命令测试：

```
C1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
PC1#
PC1#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1  *  *  *
 2  *  *  *
 3  *  *  *
.....
```

批注 [stanley614]：由于 PC1 使用 R1 作为其下一跳，所以 R1 的出错，直接导致 PC1 无法到达目标网络。

```
PC2#ping 10.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/128/160 ms
PC2#
PC2#tr
PC2#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

  1 192.168.1.2 112 msec *  96 msec
PC2#
```

批注 [stanley615]：由于 PC2 的默认网关并不是 R1 路由器，因此 R1 路由出错，不会影响 PC2 的主机。

6、虽然有两台路由器都可以到达目标网络，但是默认情况下，并没有充分利用冗余设备，因此当网络单点出错时，必然会引起部分用户无法访问网络。

7、为了解决这一问题，在 R1 和 R2 上配置 VRRP 协议，配置如下：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#vrrp 1 ip 192.168.1.1
R1(config-if)#vrrp 1 priority 200
R1(config-if)#vrrp 1 preempt
R1(config-if)#
R1(config-if)#vrrp 2 ip 192.168.1.2
R1(config-if)#vrrp 2 priority 100
R1(config-if)#vrrp 2 preempt
R1(config-if)#exit
R1(config)#
```

批注 [stanley616]：配置 VRRP 组 1，其虚拟地址为 192.168.1.1，并且设定其优先级为 200。同时开启抢占特性。

批注 [stanley617]：同时为 R1 配置 VRRP 组 2，其虚拟 IP 地址为 192.168.1.2，优先级为 100，开启抢占特性。

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#vrrp 1 ip 192.168.1.1
R2(config-if)#vrrp 1 priority 100
R2(config-if)#vrrp 1 preempt
R2(config-if)#
R2(config-if)#vrrp 2 ip 192.168.1.2
R2(config-if)#vrrp 2 priority 200
R2(config-if)#vrrp 2 preempt
R2(config-if)#exit
R2(config)#exit
R2#
```

批注 [stanley618]：由于 R2 的路由器的 VRRP 组 1 的优先级为 100，因此，R1 会做为 VRRP 组 1 的 MASTER 路由器.

批注 [stanley619]：由于 R2 的 VRRP 组 2 拥有较高的优先级 200，因此 R2 会做为 VRRP 组 2 的 MASTER 路由器.

8、通过查看两台路由器的 VRRP 组汇总信息，确认不同路由器的组身份：

```
R1#show vrrp
FastEthernet0/0 - Group 1
```

```
  State is Master
  Virtual IP address is 192.168.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 255 (cfgd 200)
  Master Router is 192.168.1.1 (local), priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.003 sec

FastEthernet0/0 - Group 2
  State is Backup
  Virtual IP address is 192.168.1.2
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.1.2, priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.349 sec)

R1#
```

批注 [stanley620]: MASTER 路由器负责组的路由。

```
R2#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.1.1, priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.773 sec)

FastEthernet0/0 - Group 2
  State is Master
  Virtual IP address is 192.168.1.2
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 255 (cfgd 200)
  Master Router is 192.168.1.2 (local), priority is 255
```

批注 [stanley621]: R2 路由器负责组 2 的路由。

```
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.003 sec

R2#
```

9、再次把 R1 路由器的 Fa0/0 接口置为 DOWN 状态， 两台路由器将会出现如下信息：

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#shutdown
R1(config-if)#
*Jul  8 21:49:59.131: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Master -> Init
*Jul  8 21:49:59.135: %VRRP-6-STATECHANGE: Fa0/0 Grp 2 state Backup -> Init
```

批注 [stanley622]: R1 路由器进入 Init 状态，并且丢失 MASTER 身份。

```
R2#
*Jul  8 21:50:03.191: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Backup -> Master
R2#
```

批注 [stanley623]: R2 路由器的 FA0/0 接口进入 MASTER 状态，表明，此时 R2 路由器已经发现 R1 路由出错。并且接替 R1 路由器的组 1 的路由工作。

10、再次在 R1 和 R2 上使用 ping 和 traceroute 确认：

```
PC1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/78/96 ms
PC1#
PC1#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

  1 192.168.1.2 92 msec *  120 msec
PC1#
```

批注 [stanley624]: 此到达 10.1.1.1 目标网络下一跳已经变更为 R2 路由器。

```
PC2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/172/452 ms
PC2#
PC2#traceroute 10.1.1.1

Type escape sequence to abort.
```

```
Tracing the route to 10.1.1.1


 1 192.168.1.2 132 msec *  168 msec
PC2#
```

11、由于在网络中启用了两个不同的 VRRP 组，所以最大限度上确保了网络冗余。同时为了更好的观察 VRRP 的工作过程，建议在 R1 和 R2 路由器上使用扩展的 PING 命令持续向目标网络发送数据包。同时在 R1 和 R2 路由器使用如下命令进行调试，具体不再列出：

```
debug vrrp events
debug vrrp packets
```

12、实验完成。

CCNP Lab Manual

Implementing Secure Converged Wide Area Networks

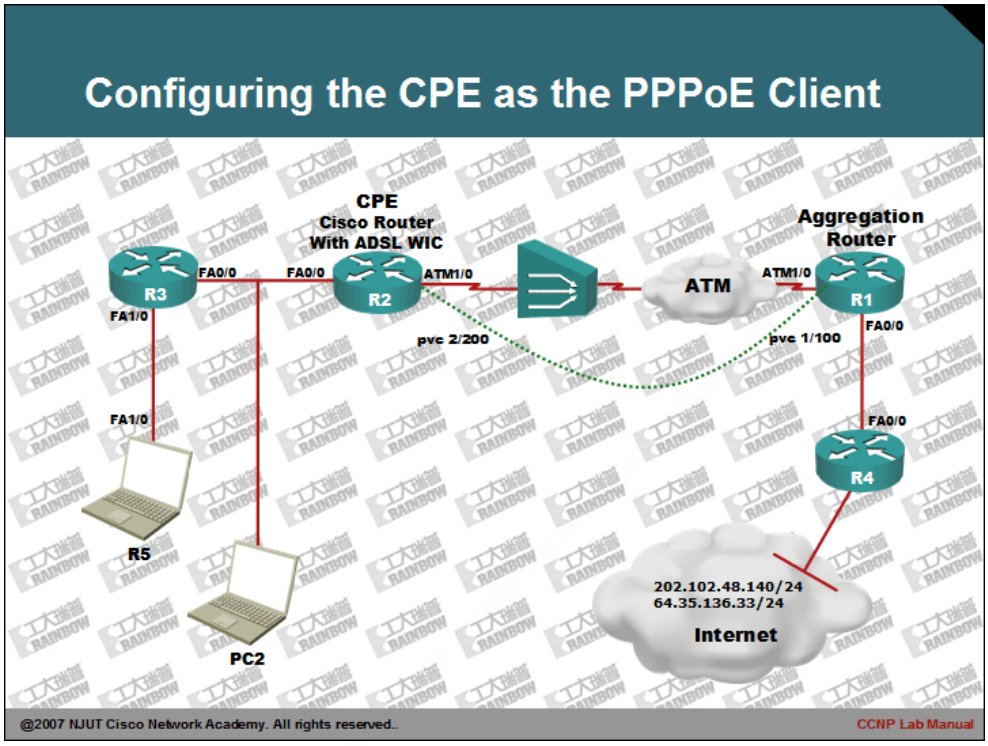
CCNP Lab Manual

Lab 59. Configuring the CPE as the PPPoE Client

实验目的：

1、掌握 PPPoE 的客户端配置方法.

实验拓扑图：



实验步骤及要求：

1、由于本实验需要模拟 ADSL 的 ISP 端的配置。而 ISP 端的配置并不需要 NP 学员掌握。因此，本处仅给出配置和简单的解释。

2、拓扑中的 R4 路由器配置。

```
R4(config)#interface loopback 0
R4(config-if)#ip address 202.102.48.140 255.255.255.0
R4(config-if)#ip address 64.35.136.33 255.255.255.0 secondary
R4(config-if)#exit
R4(config)#
R4(config)#interface fastEthernet 0/0
R4(config-if)#pppoe enable
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#
R4(config)#ip dhcp pool cisco
R4(dhcp-config)#network 211.95.36.0 /24
R4(dhcp-config)#dns-server 211.95.36.1
R4(dhcp-config)#exit
R4(config)#
R4(config)#ip dhcp excluded-address 211.95.36.1
R4(config)#
R4(config)#interface virtual-template 1
R4(config-if)#encapsulation ppp
R4(config-if)#ppp authentication chap
R4(config-if)#peer default ip address dhcp-pool cisco
R4(config-if)#ip address 211.95.36.1 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#
R4(config)#vpdn enable
R4(config)#vpdn-group 1
R4(config-vpdn)#accept-dialin
R4(config-vpdn-acc-in)#protocol pppoe
R4(config-vpdn-acc-in)#virtual-template 1
R4(config-vpdn-acc-in)#exit
R4(config-vpdn)#exit
R4(config)#
R4(config)#username adsl password cisco
R4(config)#
```

批注 [stanley625]： 配置回环口用于模拟 Internet 网络。

批注 [stanley626]： 配置 fa0/0 的接口启用 pppoe 协议。

批注 [stanley627]： 配置 DHCP 服务器，并命令为 cisco。

批注 [stanley628]： 指定 DHCP 的地址池。

批注 [stanley629]： 为客户端指点派 DNS 地址。

批注 [stanley630]： 由 211.95.36.1 地址被分配给虚拟模板，因此在此处需要排除该地址。

批注 [stanley631]： 配置虚拟模板用于实施对于客户端的身份验证。
1. 启用 PPP 的协议。
2. 选择 chap 认证方法。
3. 为客户端分配 IP 地址，并且指定其使用哪一个 DHCP 地址池。
4. 配置虚拟模板的 IP 地址。

批注 [stanley632]： 启用 VPDN。
并配置 VPDN 的组 1，指出接受客户端呼叫。并且采用 PPPOE 的协议。同时使用虚拟模板 1 的参数与客户端协商。

批注 [stanley633]： 配置本地用户名和密码数据库。以便于客户端登录。

3、拓扑中 R1 路由器配置。由于 Dynamips 目前使用的 ATM 接口不支持 PPPOE，所以只能将 R1 作为桥接设备，将数据帧桥接给 R4，由 R4 的以太口来处理 PPPOE

数据帧，下面是 R1 的桥接配置：

```
R1(config)#no ip routing
R1(config)#
R1(config)#interface fastEthernet 0/0
R1(config-if)#bridge-group 1
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#interface atM 1/0
R1(config-if)#bridge-group 1
R1(config-if)#pvc 1/100
R1(config-if-atm-vc)#encapsulation aal5snap
R1(config-if-atm-vc)#exit
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#bridge 1 protocol ieee
R1(config)#exit
R1#
```

批注 [stanley634]： 由于需要将 R1 路由器配置成 2 层的桥设备，因此建议关键路由功能。

批注 [stanley635]： 将 fa0/0 接口加入到桥接组 1。

批注 [stanley636]： 将 ATM1/0 接口加入到桥接组 1。

批注 [stanley637]： 为 ATM 的 PVC 虚拟路配置封闭协议。

批注 [stanley638]： 配置桥接组的类型，为 IEEE 标准。

4、配置拓扑中的 CPE 设备 R2 路由器：

```
R2(config)#no ip routing
R2(config)#
R2(config)#interface fastEthernet 0/0
R2(config-if)#bridge-group 1
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#interface atM 1/0
R2(config-if)#bridge-group 1
R2(config-if)#pvc 2/200
R2(config-if-atm-vc)#encapsulation aal5snap
R2(config-if-atm-vc)#exit
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#bridge 1 protocol ieee
R2(config)#exit
R2#
```

批注 [stanley639]： CPE 在此处的主要作用就是将客端的 PPPOE 数据包桥接给聚合路由器。因此无需要三层路由功能。

5、在 R2 与 R1 路由器上检测 ATM 接口，确认 ATM 可以正常工作：

```
R2#ping atm interface atM 1/0 2 200

Type escape sequence to abort.
```

```
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/92/240 ms
R2#
```

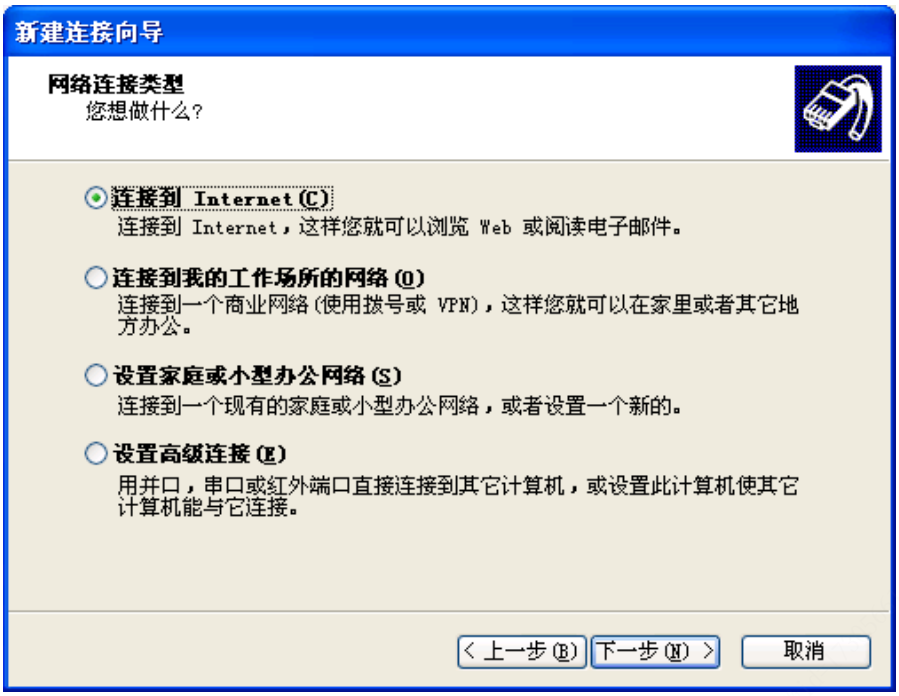
```
R1#ping atm interface aTM 1/0 1 100

Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/100/252 ms
R1#
```

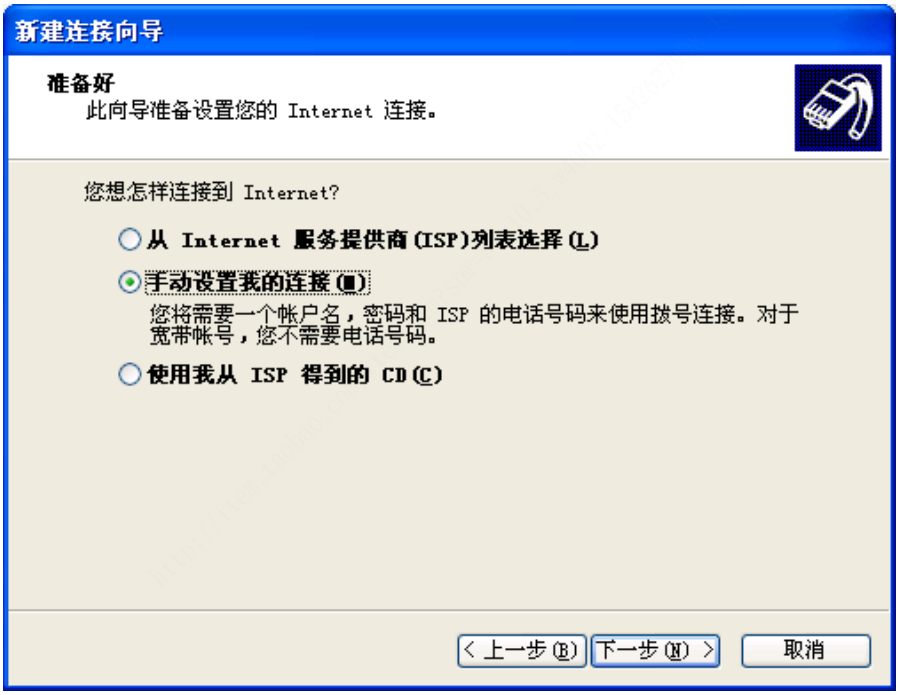
6、当完成上面 ISP 端的配置后，则可以在 PC2 主机上进行测试了，此处的 PC2 为本地网络里任一主机。PC2 的操作系统为 Windows XP。

7、在 PC2 上新建一个网络连接。在连接向导中，点击下一步。如下面所示：

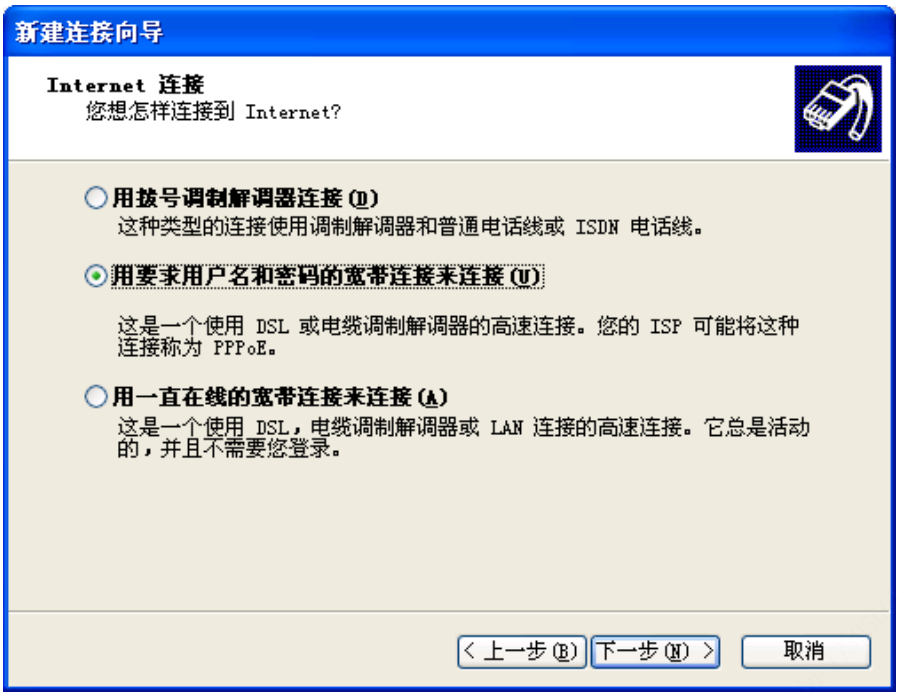
8、选择“连接到 Internet”，如下图所示：



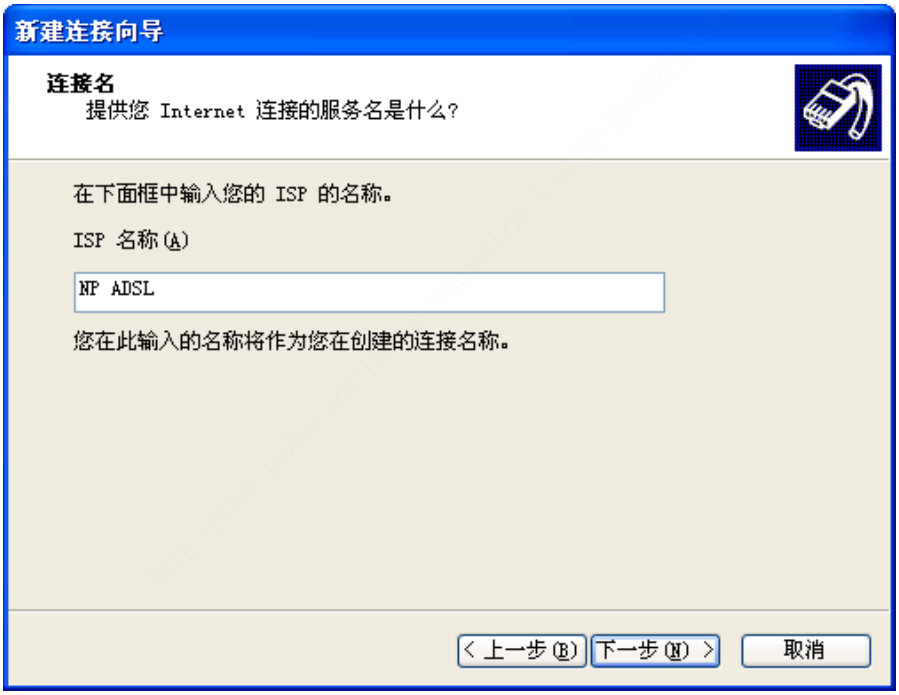
9、选择“手动设置我的连接”，点击下一步，如下图所示：



10、选择“用要求用户我和密码的宽带连接来连接”，点击下一步，如图所示：

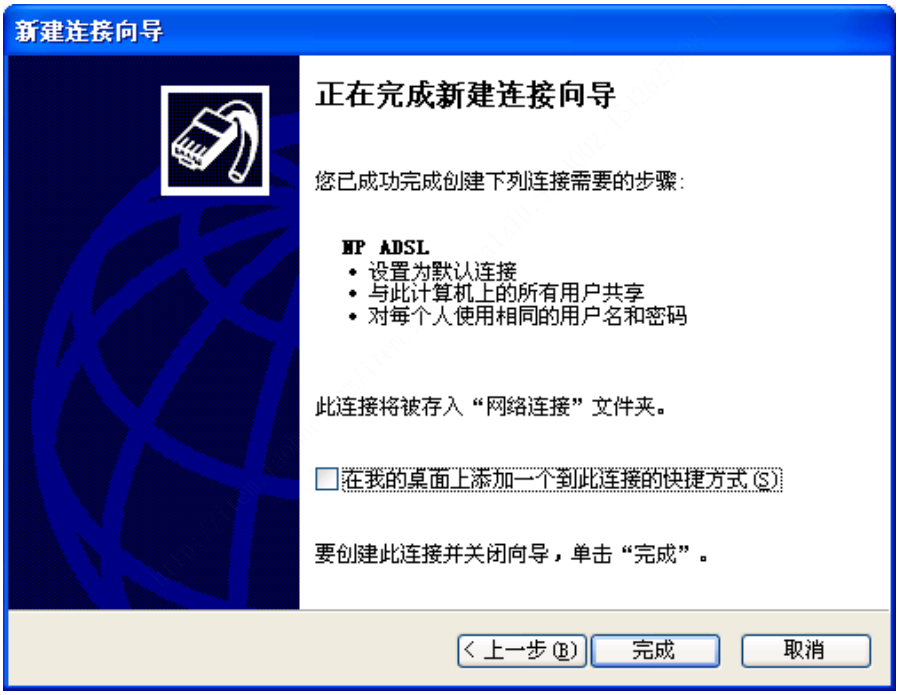


11、填写 ISP 名称，此外可以任意填写，如下图所示：



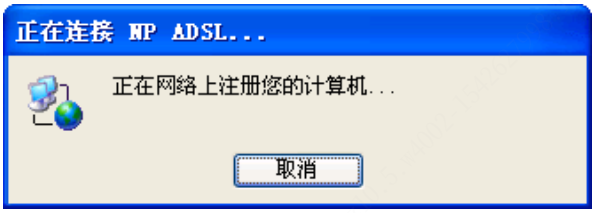
12、填写相应的 PPPoE 帐号和密码，如下图所示：

13、完成新建连接配置。



14、双击新建的 ADSL 的 PPPoE 连接，进行拨号测试，如下图所示：

15、点击拨号会出现如下信息，指出配置成功，XP 的 PPPoE 客户端可以正确的连接到 ADSL 的网络。



16、查看 XP 客户端的 IP 配置信息：

```
C:\>ipconfig /all
PPP adapter NP ADSL:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Physical Address. . . . . . . . . : 00-53-45-00-00-00
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 211.95.36.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 211.95.36.4
        DNS Servers . . . . . . . . . . . : 211.95.36.1
        NetBIOS over Tcpip. . . . . . . . : Disabled
C:\>
```

批注 [stanley640]：从聚合路由器获得的 IP 地址。

批注 [stanley641]：由聚合路由器分配的 DNS 地址。

17、使用 XP 主机使用 ping 命令确认可以连接到 Internet 网络：

```
C:\>ping 64.35.136.33
```

```
Pinging 64.35.136.33 with 32 bytes of data:

Reply from 64.35.136.33: bytes=32 time=148ms TTL=255
Reply from 64.35.136.33: bytes=32 time=15ms TTL=255
Reply from 64.35.136.33: bytes=32 time=31ms TTL=255
Reply from 64.35.136.33: bytes=32 time=265ms TTL=255

Ping statistics for 64.35.136.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 15ms, Maximum = 265ms, Average = 72ms

C:\ >
```

18、上面的配置是在 XP 的环境中完成，其主要的优点，就是能够使用 XP 的 PPPoE 客户端软件，快速的测试骨干网络的配置的正确性。下面给出了 R3 路由器的 PPPoE 客户端以及相关的 NAT 与 DHCP 的配置。

19、在 R3 上配置 DHCP 用于向客户端分配 IP。

```
R3(config)#
R3(config)#ip dhcp pool local_net
R3(dhcp-config)#network 192.168.1.0 /24
R3(dhcp-config)#default-router 192.168.1.1
R3(dhcp-config)#import all
R3(dhcp-config)#exit
R3(config)#
R3(config)#interface fastEthernet 1/0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
```

批注 [stanley642]：导入 R3 路由器从上级 DHCP 获得的 IP 配置。比如此处会将从聚合路由获得的 DNS 服务器，分配给向本地其它 DHCP Client。

20、在 R5 上配置接口为自动获取 IP 方式：

```
R5(config)#interface fastEthernet 1/0
R5(config-if)#ip address dhcp
R5(config-if)#no shutdown
R5(config-if)#exit
R5(config)#exit
```

21、配置完 R5 后，稍等片刻，会得到如下 IOS 提示：

```
R5#
*Jul  7 18:53:50.639: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet1/0 assigned DHCP address
192.168.1.2, mask 255.255.255.0, hostname R5
```

批注 [stanley643]：指出已经从 DHCP 服务器获得 IP 配置。

```
R5#
```

22、查看 R5 路由器的 IP 信息：

```
R5#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet1/0            192.168.1.2     YES DHCP   up                    up
R5#
```

批注 [stanley644]：自动获取 IP 地址。

23、使用 PING 命令测试网络连接：

```
R5#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/28/56 ms
R5#
```

24、配置 R3 路由器的 PPPoE 客户端，具体配置如下：

```
R3(config)#interface fastEthernet 0/0
R3(config-if)#pppoe enable
R3(config-if)#pppoe-client dial-pool-number 1
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
R3(config)#vpdn enable
R3(config)#
R3(config)#vpdn-group 1
R3(config-vpdn)#request-dialin
R3(config-vpdn-req-in)#protocol pppoe
R3(config-vpdn-req-in)#exit
R3(config-vpdn)#exit
R3(config)#dialer-list 1 protocol ip permit
R3(config-if)#
R3(config)#interface dialer 1
R3(config-if)#
R3(config-if)#encapsulation ppp
R3(config-if)#ppp chap hostname adsl
R3(config-if)#ppp chap password cisco
R3(config-if)#ip address negotiated
R3(config-if)#dialer pool 1
R3(config-if)#dialer-group 1
R3(config-if)#ip mtu 1496
R3(config-if)#exit
R3(config)#
```

批注 [stanley645]：将 fa0/0 接口加入到拨号池 1。

批注 [stanley646]：配置 PPPoE 客户端为请求拨号。

批注 [stanley647]：配置感兴趣数据流，以便于触发拨号。

批注 [stanley648]：启用拨号配置 1。

批注 [stanley649]：配置认证的帐号和密码。

批注 [stanley650]：配置 IP 地址为协商方式。

批注 [stanley651]：加入到拨号池 1。

批注 [stanley652]：引用拨号兴趣流，用于触发拨号。

批注 [stanley653]：配置接口的 MTU，因为 PPPoE 会给帧封装 8 个字节的报头。配置此命令主要是避免产生小巨帧，而导致传输出错。

25、配置 R3 路由器的 PAT：

```
R3(config)#interface fastEthernet 1/0
R3(config-if)#ip nat inside
R3(config-if)#exit
R3(config)#
R3(config)#interface dialer 1
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#
R3(config)#access-list 1 permit any
R3(config)#
R3(config)#ip nat inside source list 1 interface dialer 1 overload
R3(config)#
R3(config)#ip route 0.0.0.0 0.0.0.0 dialer 1
```

批注 [stanley654]：配置默认静态路由，指出默认网关。

26、在 R5 上测试，是否可以 PING 通 Internet 网络的 IP：

```
R5#ping 202.102.48.140

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.140, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/96/128 ms
R5#
R5#ping 64.35.136.33

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.35.136.33, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/112/148 ms
R5#
```

27、查看 R3 路由器的 NAT 转换表：

```
R3#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 211.95.36.3:2     192.168.1.2:2      202.102.48.140:2   202.102.48.140:2
icmp 211.95.36.3:3     192.168.1.2:3      64.35.136.33:3     64.35.136.33:3
R3#
```

28、查看 R3 的 DHCP 地址分配信息：

```
R3#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
```

```
192.168.1.2          0063.6973.636f.2d63.     Jul 08 2007 06:53 PM    Automatic
                     6130.342e.3066.6563.
                     2e30.3031.632d.4661.
                     312f.30
R3#
```

29、查看 PPPoE 会话信息：

```
R3#show pppoe session
Total PPPoE sessions 1


PPPoE Session Information
UID     SID     RemMAC          OIntf           Intf       Session
                LocMAC                          VASt       state
0       2       ca03.0fec.0000 Fa0/0            Vi1        N/A
                ca02.0fec.0000                  UP
R3#
```

30、实验完成。

CCNP Lab Manual

Lab 60. Configuring GRE Tunnels

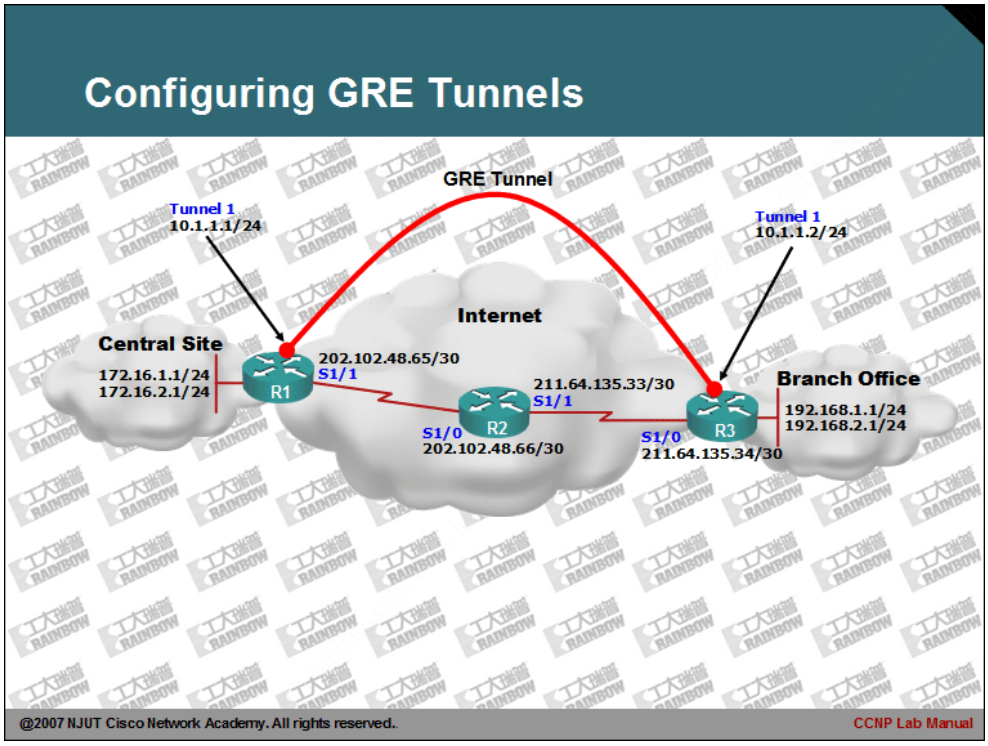
实验目的：

1、掌握 GRE 隧道配置。

2、GRE 隧道本身并不支持数据加密。需要其它协议如 IPsec 等实现数据传输加密。

3、GRE 支持广播。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、在 R1 和 R3 上配置静态路由。确保 Internet 网络骨干可以相互通信。

```
R1(config)#ip route 0.0.0.0 0.0.0.0 202.102.48.66
```

```
R3(config)#ip route 0.0.0.0 0.0.0.0 211.64.135.33
```

在 R1 与 R3 上配置静态默认数由，不仅仅是用于模拟接入路由器。同时还为了确保在创建隧道时，隧道源与隧道目标的 IP 地址相互可见。以便于实现隧道。

3、确认 R1 能够 Ping 通 R3 路由器的公网接口 IP。

```
R1#ping 211.64.135.34

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 211.64.135.34, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/204/264 ms
R1#
```

4、在 R1 或 R3 路由器上 Ping 路由器 R3 或 R1 的回环口。

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R1#
```

批注 [stanley655]: R1 路由器使用默认路由将到达 192.168.1.1/24 的 ICMP 的数据包转发给 R2 路由器。由于 R2 路由器处于 Internet 骨干没有到达私有网络的路由。因此处会收到 U，即 R2 路由器的 ICMP 返回的不可达信息。

5、在 R1 路由器上配置 GRE 隧道。

```
R1(config)#interface tunnel 0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#tunnel source serial 1/1
R1(config-if)#tunnel destination 211.64.135.34
R1(config-if)#exit
R1(config)#
```

批注 [stanley656]: 启用 GRE 隧道。

批注 [stanley657]: 为隧道指定 IP 地址。

批注 [stanley658]: 配置隧道的本地源端口。

批注 [stanley659]: 配置隧道的目标出口。
目的端口的 IP 地址可达性，是通过本地配置的默认路由保证的。

6、在 R3 路由器上配置 GRE 隧道。

```
R3(config)#interface tunnel 0
R3(config-if)#ip address 10.1.1.2 255.255.255.0
R3(config-if)#tunnel source serial 1/0
R3(config-if)#tunnel destination 202.102.48.65
R3(config-if)#exit
```

```
R3(config)#exit
```

7、在 R1 上查看隧道接口信息。

```
R1#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.1.1.1/24
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 202.102.48.65 (Serial1/1), destination 211.64.135.34
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
.....
R1#
```

批注 [stanley660]：当 R1 和 R3 方配置好隧道后，在本地查看隧道接口，其状态应为 up。

批注 [stanley661]：基于隧道的接口。

批注 [stanley662]：采用了 GRE 隧道协议进行数据的封装。即在原始的数据包基础上，再次封装一个 GRE 的报头。

批注 [stanley663]：隧道的协议为 GRE。

8、查看 R1 的路由表。

```
R1#show ip route

Gateway of last resort is 202.102.48.66 to network 0.0.0.0

     202.102.48.0/30 is subnetted, 1 subnets
C       202.102.48.64 is directly connected, Serial1/1
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Tunnel0
S*   0.0.0.0/0 [1/0] via 202.102.48.66
R1#
```

批注 [stanley664]：隧道接口的直连路由。

9、在 R1 上 PING 路由器 R3 的隧道接口。

```
R1#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/169/264 ms
R1#
```

10、在 R1 和 R3 分别配置目标为 R1 和 R3 的回环接口，下一跳为隧道接口的路由。

```
R1(config)#ip route 192.168.0.0 255.255.0.0 10.1.1.2
```

```
R3(config)#ip route 172.16.0.0 255.255.0.0 10.1.1.1
```

11、再次在 R1 或是 R3 上使用 PING 命令，检测是否可以 PING 对方的环回接口的私有网络地址。

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 140/178/248 ms
R1#
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/164/216 ms
R1#
```

12、还可以使用如下命令，查看 GRE 隧道的其它信息。

```
R1#show interfaces tunnel 0 stats
Tunnel0
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor         15       1860         15       1860
             Route cache          0        360          0          0
                   Total         15       2220         15       1860
R1#
```

13、实验完成。

CCNP Lab Manual

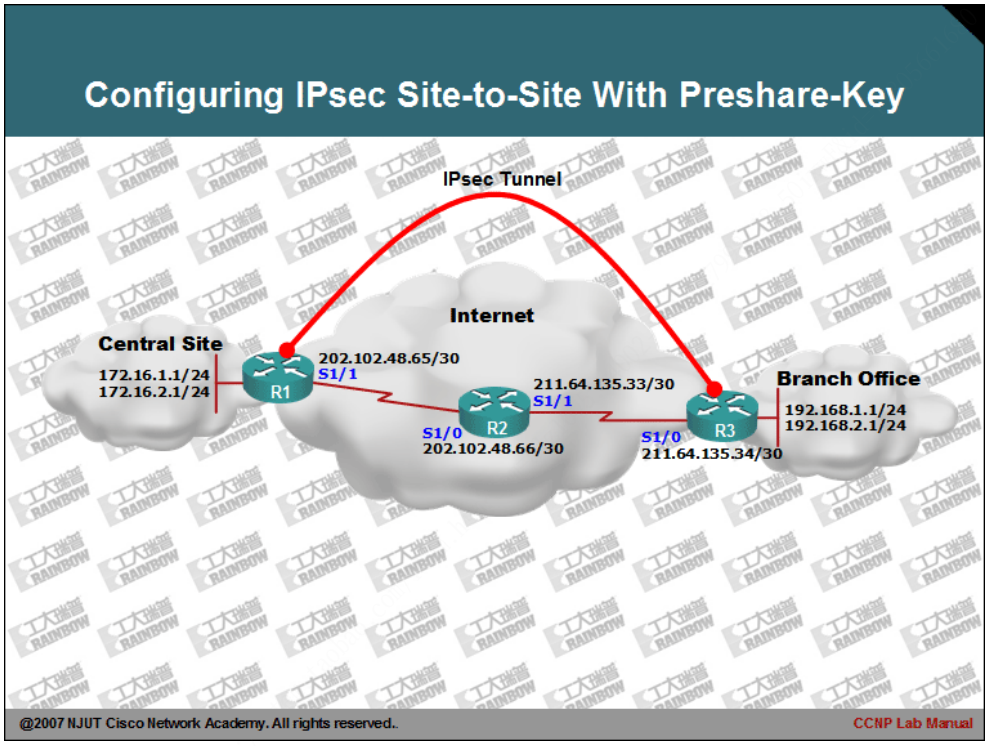
Lab 61. Configuring IPsec Site-to-Site With Preshare-Key

实验目的：

1、掌握 IPsec 隧道配置。

2、深刻理解 IKE 阶段 1 与阶段 2 的协商过程。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、在 R1 和 R3 上配置静态路由。确保 Internet 网络骨干可以相互通信。

```
R1(config)#ip route 0.0.0.0 0.0.0.0 202.102.48.66
```

```
R3(config)#ip route 0.0.0.0 0.0.0.0 211.64.135.33
```

3、在 R1 路由器上配置 IKE 阶段一需要使用策略。

```
R1(config)#crypto isakmp enable
```

4、配置预共享密钥,在两台对等体路由器上密钥必须一致。

```
R1(config)#crypto isakmp key 0 ciscokey address 211.64.135.34
```

5、为 IKE 阶段一的协商，配置 ISAKMP 的策略。可以在本地配置多个 ISAKMP 的策略，在与对等体协商，会选择一个匹配策略，而不管策略的编号。

```
R1(config)#
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#hash md5
R1(config-isakmp)#encryption des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#group 1
R1(config-isakmp)#exit
R1(config)#
```

6、配置 IPsec 变换集,其用于 IKE 阶段二的 IPsec 的 SA 协商。指定协商的加密参数。

其包含了安全和压缩协议、散列算法和加密算法。

本配置使用了 esp 与 des 的协作的认证加密算法，实现对数据的保护。并且指定其用于隧道模式。

```
R1(config)#crypto ipsec transform-set my_trans esp-des
R1(cfg-crypto-trans)#mode tunnel
R1(cfg-crypto-trans)#exit
R1(config)#
```

7、配置加密访问控制列表，用于指出那些数据流是需要加密的，有时也被称为定义 IPsec 的感兴趣流。

通过 ACL 配置，标识出从本地到达 192.168.0.0/16 网络的所有 IP 数据包均会

批注 [stanley665]: 在 R1 路由器上启用 ISAKMP。
在新版本 ISAKMP 默认是开启的。

批注 [stanley666]: 其中 0 表示使用一个未加密的密钥。如果想使用加密的密钥，需要使用 6 的配置选项。

ciscokey 为配置的密钥。

address 标识了对等体是谁。也可以使用 hostname 进行配置。

批注 [stanley667]:
启用 ISAKMP

配置散列算法为 md5，其用于确保数据完整性。MD5 的算法是理论上是不可逆的。

指定加密算法为 DES，还有 3DES 和 AES 等选项。
DES 一种对称的加密算法。

认证方法使用预共享密钥进行认证。

lifetime 指出协商后的 SA 的寿命。

配置使用 DH 组 1 进行密钥交换。
DH1/2 密钥长度：768/1024
DH 还有组 5 和组 7 。

被加密并且从 IPsec 隧道中通过。

```
R1(config)#access-list 100 permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.255.255
R1(config)#
```

8、配置加密映射表，用于关联相关的变换集。

```
R1(config)#crypto map vpn_to_R3 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 211.64.135.34
R1(config-crypto-map)#set transform-set my_trans
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#exit
R1#
```

批注 [stanley668]: 可以为多个对等体建立 IPsec SA，则需要在配置多个 MAP 条目。

批注 [stanley669]: 指定对等为 211.64.135.34

批注 [stanley670]: 引用之前所定义的 IPsec 的变换集。

批注 [stanley671]: 针对 acl 100 所指定的数据流进行保护。

9、将加密映射表应用到需要建立隧道接口。

```
R1(config)#interface serial 1/1
R1(config-if)#crypto map vpn_to_R3
R1(config-if)#exit
R1(config)#
```

10、在 R3 采用如上配置进行配置 IKE 阶段 1 和阶段 2。

```
R3(config)#crypto isakmp enable
R3(config)#
R3(config)#crypto isakmp key 0 ciscokey address 202.102.48.65
R3(config)#
R3(config)#crypto isakmp policy 2
R3(config-isakmp)#hash md5
R3(config-isakmp)#encryption des
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#lifetime 86400
R3(config-isakmp)#group 1
R3(config-isakmp)#exit
R3(config)#
R3(config)#crypto ipsec transform-set my_trans esp-des
R3(cfg-crypto-trans)#mode tunnel
R3(cfg-crypto-trans)#exit
R3(config)#
R3(config)#access-list 100 permit ip 192.168.0.0 0.0.255.255 172.16.0.0 0.0.255.255
R3(config)#
R3(config)#crypto map vpn_to_R1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 202.102.48.65
```

```
R3(config-crypto-map)#set transform-set my_trans
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#interface serial 1/0
R3(config-if)#crypto map vpn_to_R1
R3(config-if)#exit
R3(config)#
```

11、在 R1 路由器打开 ISAKMP 的调试。

```
R1#
R1#debug crypto isakmp
Crypto ISAKMP debugging is on
R1#
R1#debug crypto ipsec
Crypto IPSEC debugging is on
R1#
```

12、确认 R1 和 R3 的 ISAKMP 的策略。

```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
R1#
```

批注 [stanley672]：自定义的 ISAKMP 的策略设置。

批注 [stanley673]：默认的系统配置的 ISAKMP 的策略

```
R3#show crypto isakmp policy

Global IKE policy
Protection suite of priority 2
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

批注 [stanley674]：R3 的 ISAKMP 自定义的策略。其配置必须要与 R1 的策略配置一致。

```
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
R3#
```

批注 [stanley675]：默认的系统配置的 ISAKMP 的策略

13、在 R1 与 R3 上查看 ISAKMP 的预共享密钥配置，并确认双方配置一致。

```
R1#show crypto isakmp key
Keyring      Hostname/Address                          Preshared Key

default      211.64.135.34                             ciscokey
R1#
```

```
R3#show crypto isakmp key
Keyring      Hostname/Address                          Preshared Key

default      202.102.48.65                             ciscokey
R3#
```

14、在 R1 与 R3 上查看 IPsec 的变换集。

```
R1#show crypto ipsec transform-set
Transform set my_trans: { esp-des  }
   will negotiate = { Tunnel,  },
R1#
```

批注 [stanley676]：隧道方式。

```
R3#show crypto ipsec transform-set
Transform set my_trans: { esp-des  }
   will negotiate = { Tunnel,  },
R3#
```

15、在 R1 上使用扩展命令去 ping 路由器 R2 回环口的私有地址。

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
```

批注 [stanley677]：指定源地址，其源地址必须与 ACL 所指定的源地址相匹配。

批注 [stanley678]：指定目标地址。也必须与 ACL 所匹配。否则不能触发 ISAKMP 的协商。

```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1

*Jun  5 17:08:59.519: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 202.102.48.65, remote= 211.64.135.34,
    local_proxy= 172.16.0.0/255.255.0.0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.0.0/0 (type=4),
    protocol= ESP, transform= NONE  (Tunnel),
    lifedur= 3600s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
*Jun  5 17:08:59.535: ISAKMP:(0): SA request profile is (NULL)
*Jun  5 17:08:59.539: ISAKMP: Created a peer struct for 211.64.135.34, peer port 500
*Jun  5 17:08:59.539: ISAKMP: New peer created peer = 0x653F9630 peer_handle = 0x80000005
*Jun  5 17:08:59.543: ISAKMP: Locking peer struct 0x653F9630, refcount 1 for isakmp_initiator
*Jun  5 17:08:59.547: ISAKMP: local port 500, remote port 500
*Jun  5 17:08:59.547: ISAKMP: set new node 0 to QM_IDLE
*Jun  5 17:08:59.551: insert sa successfully sa = 65D68724
*Jun  5 17:08:59.555: ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
*Jun  5 17:08:59.555: ISAKMP:(0):found peer pre-shared key matching 211.64.135.34
*Jun  5 17:08:59.559: ISAKMP:(0): constructed NAT-T vendor-07 ID
*Jun  5 17:08:59.559: ISAKMP:(0): constructed NAT-T vendor-03 ID
*Jun  5 17:08:59.559: ISAKMP:(0): constructed NAT-T vendor-02 ID
*Jun  5 17:08:59.559: ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
*Jun  5 17:08:59.559: ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1

*Jun  5 17:08:59.559: ISAKMP:(0): beginning Main Mode exchange
*Jun  5 17:08:59.559: ISAKMP:(0): sending packet to 211.64.135.34 my_port 500 peer_port 500
(I) MM_NO_STATE
*Jun  5 17:08:59.663: ISAKMP (0:0): received packet from 211.64.135.34 dport 500 sport 500
Global (I) MM_NO_STATE
*Jun  5 17:08:59.671: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun  5 17:08:59.671: ISAKMP:(0):Old State = IKE_I_MM1  New State = IKE_I_MM2

*Jun  5 17:08:59.683: ISAKMP:(0): processing SA payload. message ID = 0
*Jun  5 17:08:59.687: ISAKMP:(0): processing vendor id payload
*J.
Success rate is 80 percent (4/5), round-trip min/avg/max = 36/53/64 ms
R1#un  5 17:08:59.687: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
*Jun  5 17:08:59.691: ISAKMP (0:0): vendor ID is NAT-T v7
```

批注 [stanley679]： IKE 阶段一默认会采用积极模式进行协商。

批注 [stanley680]： 发现对等体所配置的密钥，与本地配置的密钥时匹配的。

预共享密钥，主要目的是确认对等体是可信任的。

后面会发现多个预共享密钥被发现信息。其目的是每个协商数据包都会携带密钥。以确保对等体可信。

批注 [stanley681]： 开始主动模式交换。

批注 [stanley682]： ISAKMP 默认使用 UDP 的 500 号端口与对等体进行协商。

```
*Jun  5 17:08:59.691: ISAKMP:(0):found peer pre-shared key matching 211.64.135.34
*Jun  5 17:08:59.695: ISAKMP:(0): local preshared key found
*Jun  5 17:08:59.695: ISAKMP : Scanning profiles for xauth ...
*Jun  5 17:08:59.699: ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
*Jun  5 17:08:59.699: ISAKMP:       encryption DES-CBC
*Jun  5 17:08:59.703: ISAKMP:       hash MD5
*Jun  5 17:08:59.703: ISAKMP:       default group 1
*Jun  5 17:08:59.707: ISAKMP:       auth pre-share
*Jun  5 17:08:59.711: ISAKMP:       life type in seconds
*Jun  5 17:08:59.711: ISAKMP:       life duration (VPI) of  0x0 0x1 0x51 0x80
*Jun  5 17:08:59.719: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun  5 17:08:59.723: ISAKMP:(0): processing vendor id payload
*Jun  5 17:08:59.723: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
*Jun  5 17:08:59.727: ISAKMP (0:0): vendor ID is NAT-T v7
*Jun  5 17:08:59.727: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Jun  5 17:08:59.727: ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM2

*Jun  5 17:08:59.727: ISAKMP:(0): sending packet to 211.64.135.34 my_port 500 peer_port 500
(I) MM_SA_SETUP
*Jun  5 17:08:59.727: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Jun  5 17:08:59.731: ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3

*Jun  5 17:08:59.951: ISAKMP (0:0): received packet from 211.64.135.34 dport 500 sport 500
Global (I) MM_SA_SETUP
*Jun  5 17:08:59.959: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun  5 17:08:59.959: ISAKMP:(0):Old State = IKE_I_MM3  New State = IKE_I_MM4
*Jun  5 17:08:59.975: ISAKMP:(0): processing KE payload. message ID = 0
*Jun  5 17:09:00.007: ISAKMP:(0): processing NONCE payload. message ID = 0
*Jun  5 17:09:00.007: ISAKMP:(0):found peer pre-shared key matching 211.64.135.34
*Jun  5 17:09:00.019: ISAKMP:(1001): processing vendor id payload
*Jun  5 17:09:00.019: ISAKMP:(1001): vendor ID is Unity
*Jun  5 17:09:00.023: ISAKMP:(1001): processing vendor id payload
*Jun  5 17:09:00.023: ISAKMP:(1001): vendor ID is DPD
*Jun  5 17:09:00.027: ISAKMP:(1001): processing vendor id payload
*Jun  5 17:09:00.031: ISAKMP:(1001): speaking to another IOS box!
*Jun  5 17:09:00.031: ISAKMP:(1001):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Jun  5 17:09:00.031: ISAKMP:(1001):Old State = IKE_I_MM4  New State = IKE_I_MM4
*Jun  5 17:09:00.031: ISAKMP:(1001):Send initial contact
*Jun  5 17:09:00.031: ISAKMP:(1001):SA is doing pre-shared key authentication using id type
ID_IPV4_ADDR
*Jun  5 17:09:00.031: ISAKMP (0:1001): ID payload
        next-payload : 8
        type         : 1
```

批注 [stanley683]： 发现对等体所配置的密钥，与本地配置的密钥时匹配的。

批注 [stanley684]： 检查本地配置的 ISAKMP 的策略。

批注 [stanley685]： 此处显示对等体所配置的 ISAKMP 策略属性是正确的。

批注 [stanley686]： 发现对等体所配置的密钥，与本地配置的密钥时匹配的。

批注 [stanley687]： 此处信息显示 IKE 阶段一的安全关联已经创建成功。

后续信息陆续显示 IKE 的一些其它的协商信息。

```
        address       : 202.102.48.65
        protocol      : 17
        port          : 500
        length        : 12
*Jun  5 17:09:00.031: ISAKMP:(1001):Total payload length: 12
*Jun  5 17:09:00.031: ISAKMP:(1001): sending packet to 211.64.135.34 my_port 500 peer_port
500 (I) MM_KEY_EXCH
*Jun  5 17:09:00.031: ISAKMP:(1001):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Jun  5 17:09:00.031: ISAKMP:(1001):Old State = IKE_I_MM4  New State = IKE_I_MM5
*Jun  5 17:09:00.139: ISAKMP (0:1001): received packet from 211.64.135.34 dport 500 sport 500
Global (I) MM_KEY_EXCH
*Jun  5 17:09:00.147: ISAKMP:(1001): processing ID payload. message ID = 0
*Jun  5 17:09:00.151: ISAKMP (0:1001): ID payload
        next-payload : 8
        type         : 1
        address      : 211.64.135.34
        protocol     : 17
        port         : 500
        length       : 12
*Jun  5 17:09:00.151: ISAKMP:(0):: peer matches *none* of the profiles
*Jun  5 17:09:00.151: ISAKMP:(1001): processing HASH payload. message ID = 0
*Jun  5 17:09:00.151: ISAKMP:(1001):SA authentication status:
        authenticated
*Jun  5 17:09:00.151: ISAKMP:(1001):SA has been authenticated with 211.64.135.34
*Jun  5 17:09:00.151: ISAKMP: Trying to insert a peer 202.102.48.65/211.64.135.34/500/,  and
inserted successfully 653F9630.
*Jun  5 17:09:00.151: ISAKMP:(1001):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun  5 17:09:00.151: ISAKMP:(1001):Old State = IKE_I_MM5  New State = IKE_I_MM6

*Jun  5 17:09:00.151: ISAKMP:(1001):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
*Jun  5 17:09:00.151: ISAKMP:(1001):Old State = IKE_I_MM6  New State = IKE_I_MM6

*Jun  5 17:09:00.151: ISAKMP:(1001):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
*Jun  5 17:09:00.151: ISAKMP:(1001):Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE

*Jun  5 17:09:00.151: ISAKMP:(1001):beginning Quick Mode exchange, M-ID of -544134848
*Jun  5 17:09:00.151: ISAKMP:(1001):QM Initiator gets spi
*Jun  5 17:09:00.151: ISAKMP:(1001): sending packet to 211.64.135.34 my_port 500 peer_port
500 (I) QM_IDLE
*Jun  5 17:09:00.151: ISAKMP:(1001):Node -544134848, Input = IKE_MESG_INTERNAL, IKE_INIT_QM
*Jun  5 17:09:00.151: ISAKMP:(1001):Old State = IKE_QM_READY  New State = IKE_QM_I_QM1
*Jun  5 17:09:00.151: ISAKMP:(1001):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
*Jun  5 17:09:00.151: ISAKMP:(1001):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE
```

批注 [stanley688]： 此处确定的 IKE 阶段一的协商完成。

这是因为 CISCO 的信息反馈的延迟造成的。

批注 [stanley689]： 开始 IKE 阶段二的快速模式的协商。

批注 [stanley690]： 快速模式开始协商并计算 SPI 号。

```
*Jun  5 17:09:00.299: ISAKMP (0:1001): received packet from 211.64.135.34 dport 500 sport 500
Global (I) QM_IDLE
*Jun  5 17:09:00.307: ISAKMP:(1001): processing HASH payload. message ID = -544134848
*Jun  5 17:09:00.307: ISAKMP:(1001): processing SA payload. message ID = -544134848
*Jun  5 17:09:00.311: ISAKMP:(1001):Checking IPSec proposal 1
*Jun  5 17:09:00.311: ISAKMP: transform 1, ESP_DES
*Jun  5 17:09:00.311: ISAKMP:   attributes in transform:
*Jun  5 17:09:00.311: ISAKMP:      encaps is 1 (Tunnel)
*Jun  5 17:09:00.311: ISAKMP:      SA life type in seconds
*Jun  5 17:09:00.311: ISAKMP:      SA life duration (basic) of 3600
*Jun  5 17:09:00.311: ISAKMP:      SA life type in kilobytes
*Jun  5 17:09:00.311: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
*Jun  5 17:09:00.311: ISAKMP:(1001):atts are acceptable.
*Jun  5 17:09:00.311: IPSEC(validate_proposal_request): proposal part #1
*Jun  5 17:09:00.311: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 202.102.48.65, remote= 211.64.135.34,
    local_proxy= 172.16.0.0/255.255.0.0/0/0 (type=4),
    remote_proxy= 192.168.0.0/255.255.0.0/0/0 (type=4),
    protocol= ESP, transform= esp-des  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
*Jun  5 17:09:00.311: Crypto mapdb : proxy_match
        src addr     : 172.16.0.0
        dst addr     : 192.168.0.0
        protocol     : 0
        src port     : 0
        dst port     : 0
*Jun  5 17:09:00.311: ISAKMP:(1001): processing NONCE payload. message ID = -544134848
*Jun  5 17:09:00.311: ISAKMP:(1001): processing ID payload. message ID = -544134848
*Jun  5 17:09:00.311: ISAKMP:(1001): processing ID payload. message ID = -544134848
*Jun  5 17:09:00.311: ISAKMP:(1001): Creating IPSec SAs
*Jun  5 17:09:00.311:         inbound SA from 211.64.135.34 to 202.102.48.65 (f/i)  0/ 0
        (proxy 192.168.0.0 to 172.16.0.0)
*Jun  5 17:09:00.311:         has spi 0x702868C8 and conn_id 0
*Jun  5 17:09:00.311:         lifetime of 3600 seconds
*Jun  5 17:09:00.311:         lifetime of 4608000 kilobytes
*Jun  5 17:09:00.311:         outbound SA from 202.102.48.65 to 211.64.135.34 (f/i) 0/0
        (proxy 172.16.0.0 to 192.168.0.0)
*Jun  5 17:09:00.311:         has spi  0xA9133A18 and conn_id 0
*Jun  5 17:09:00.311:         lifetime of 3600 seconds
*Jun  5 17:09:00.311:         lifetime of 4608000 kilobytes
*Jun  5 17:09:00.311: ISAKMP:(1001): sending packet to 211.64.135.34 my_port 500 peer_port
```

批注 [stanley691]： 检测 proposal 中的 IPsec 的变换集。

批注 [stanley692]： 此处显示 IPsec 的变换集确认成功。

批注 [stanley693]： IPsec 隧道方式，协议是 ESP，使用 DES 进行数据加密。

批注 [stanley694]： 此信息为入站的安全关联索引为：0x702868c8，在以后进行数据传输时，会使用此索引进行数据加密和认证的传输。

批注 [stanley695]： 此信息为出站的安全关联索引号。

```
500 (I) QM_IDLE
*Jun  5 17:09:00.311: ISAKMP:(1001):deleting node -544134848 error FALSE reason "No Error"
*Jun  5 17:09:00.311: ISAKMP:(1001):Node -544134848, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
*Jun  5 17:09:00.311: ISAKMP:(1001):Old State = IKE_QM_I_QM1  New State =
IKE_QM_PHASE2_COMPLETE
*Jun  5 17:09:00.311: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Jun  5 17:09:00.311: Crypto mapdb : proxy_match
        src addr     : 172.16.0.0
        dst addr     : 192.168.0.0
        protocol     : 0
        src port     : 0
        dst port     : 0
*Jun  5 17:09:00.311: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same
proxies and peer 211.64.135.34
*Jun  5 17:09:00.311: IPSEC(policy_db_add_ident): src 172.16.0.0, dest 192.168.0.0, dest_port
0

*Jun  5 17:09:00.311: IPSEC(create_sa): sa created,
  (sa) sa_dest= 202.102.48.65, sa_proto= 50,
    sa_spi= 0x702868C8(1881696456),
    sa_trans= esp-des , sa_conn_id= 1
*Jun  5 17:09:00.311: IPSEC(create_sa): sa created,
  (sa) sa_dest= 211.64.135.34, sa_proto= 50,
    sa_spi= 0xA9133A18(2836609560),
    sa_trans= esp-des , sa_conn_id= 2
*Jun  5 17:09:00.311: IPSEC(update_current_outbound_sa): updated peer 211.64.135.34 current
outbound sa to SPI A9133A18
!!!!
R1#
```

批注 [stanley696]: 此处信息显示 IKE 阶段二的 IPsec 的安全关联已经协商成功。

批注 [stanley697]: 已经可以与对等的环回口进行安全的数据传输。

16、查看本地的 IKE 阶段一的安全关联。

```
R1#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
211.64.135.34   202.102.48.65   QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

批注 [stanley698]: Isakmp 的 SA 处于 ACTIVE 状态。

QM 的状态积极模式.

16、查看 IKE 阶段二的 IPsec 的安全关联。

```
R1#show crypto ipsec sa
```

```
interface: Serial1/1
    Crypto map tag: vpn_to_R3, local addr 202.102.48.65
.....
      local crypto endpt.: 202.102.48.65, remote crypto endpt.: 211.64.135.34
      path mtu 1500, ip mtu 1500, ip mtu idb Serial1/1
      current outbound spi: 0xA9133A18(2836609560)

      inbound esp sas:
       spi: 0x702868C8(1881696456)
         transform: esp-des ,
         in use settings ={Tunnel, }
         conn id: 1, flow_id: 1, crypto map: vpn_to_R3
         sa timing: remaining key lifetime (k/sec): (4436970/1326)
         IV size: 8 bytes
         replay detection support: N
         Status: ACTIVE
.....
      outbound esp sas:
       spi: 0xA9133A18(2836609560)
         transform: esp-des ,
         in use settings ={Tunnel, }
         conn id: 2, flow_id: 2, crypto map: vpn_to_R3
         sa timing: remaining key lifetime (k/sec): (4436970/1325)
         IV size: 8 bytes
         replay detection support: N
         Status: ACTIVE
.....

R1#
```

批注 [stanley699]: S1/1 接口的加密图标记。

批注 [stanley700]: 进站的 SPI 号，及认证加密方法。以及相关的状态信息。

批注 [stanley701]: 出站的 SPI 号及认证加密方法。以及相关的状态信息。

17、在 R1 和 R3 路由器上再次使用扩展的 ping 命令确认 IPsec 的 site-to-site 隧道。

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
```

```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/102/140 ms
R1#
```

```
R3#ping
Protocol [ip]:
Target IP address: 172.16.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/95/144 ms
R3#
```

18、实验完成。

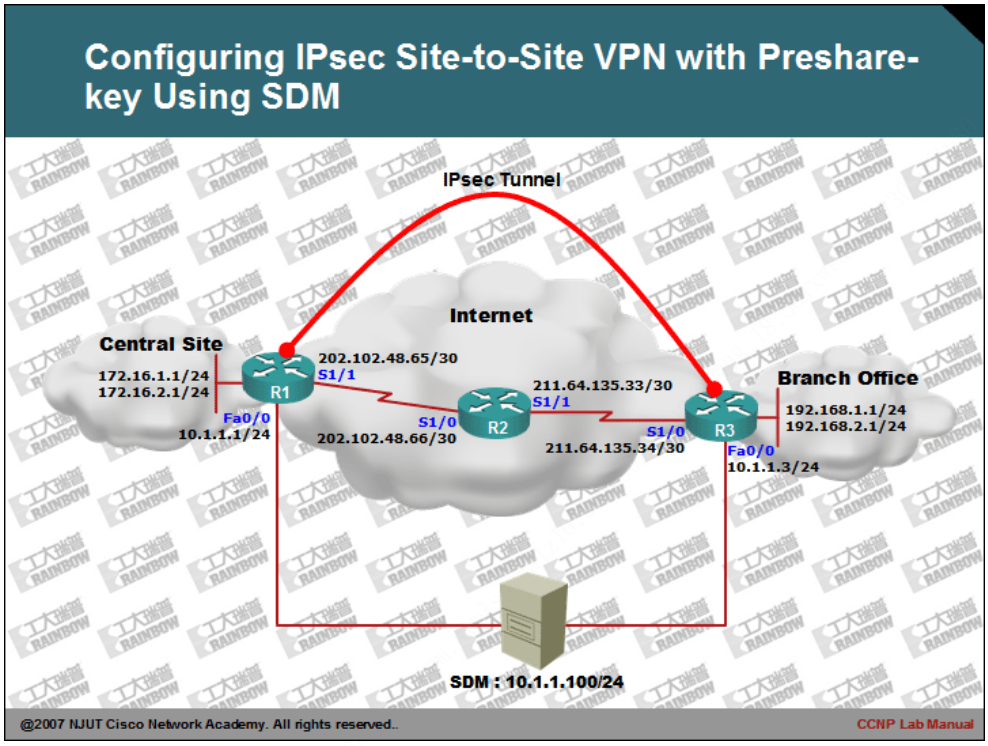
CCNP Lab Manual

Lab 62. Configuring IPsec Site-to-Site VPN Using SDM

实验目的：

1、掌握如何利用 SDM 来配置 IPsec 的 Site-to-Site VPN.

实验拓扑图：



实验步骤及要求：

1、首先在一台 PC 上安装 Cisco SDM 软件,并且需要安装 JAVA 环境。

2、配置各台路由器的 IP 地址，并且使用 ping 命令确认各路由器的直连口的互通性。基本配置如下：

```
R1(config)#interface loop 0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip address 172.16.2.1 255.255.255.0 secondary
R1(config-if)#exit
R1(config)#interface serial 1/1
R1(config-if)#ip address 202.102.48.65 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#no cdp enable
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 202.102.48.66
```

```
R2(config)#interface serial 1/0
R2(config-if)#ip address 202.102.48.66 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config-if)#
R2(config)#interface serial 1/1
R2(config-if)#ip address 211.64.135.33 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

```
R3(config)#interface loopback 0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#ip address 192.168.2.1 255.255.255.0 secondary
R3(config-if)#exit
R3(config)#interface serial 1/0
R3(config-if)#ip address 211.64.135.34 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fastethernet 0/0
R3(config-if)#no cdp enable
R3(config-if)#ip address 10.1.1.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
```

```
R3(config)#ip route 0.0.0.0 0.0.0.0 211.64.135.33
```

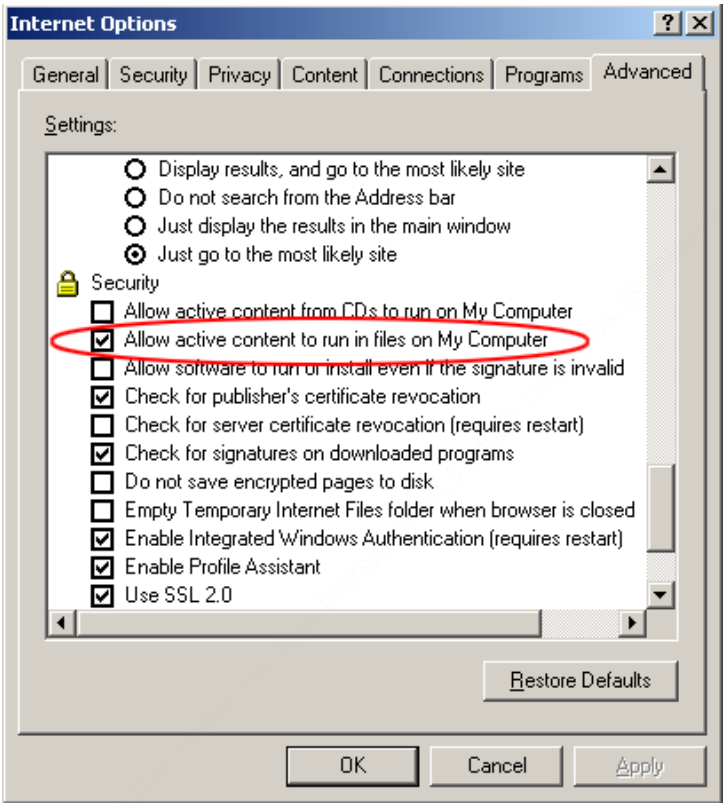
3、为了能够让SDM连接到R1和R3路由器，因此需要在R1和R3上启用http server服务，配置如下：

```
R1(config)#ip http server
```

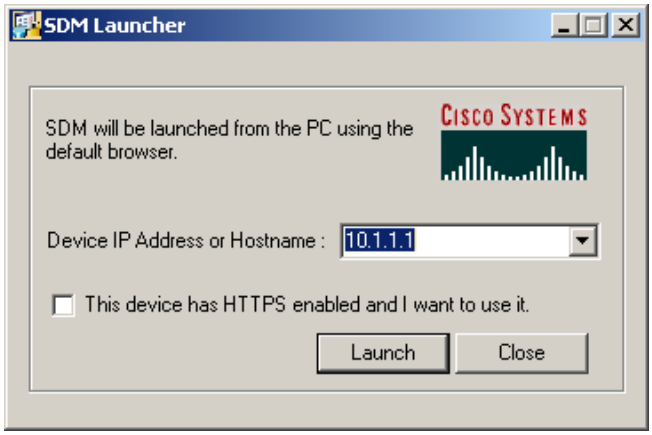
批注 [stanley702]: 启用ip http server服务。

```
R3(config)#ip http server
```

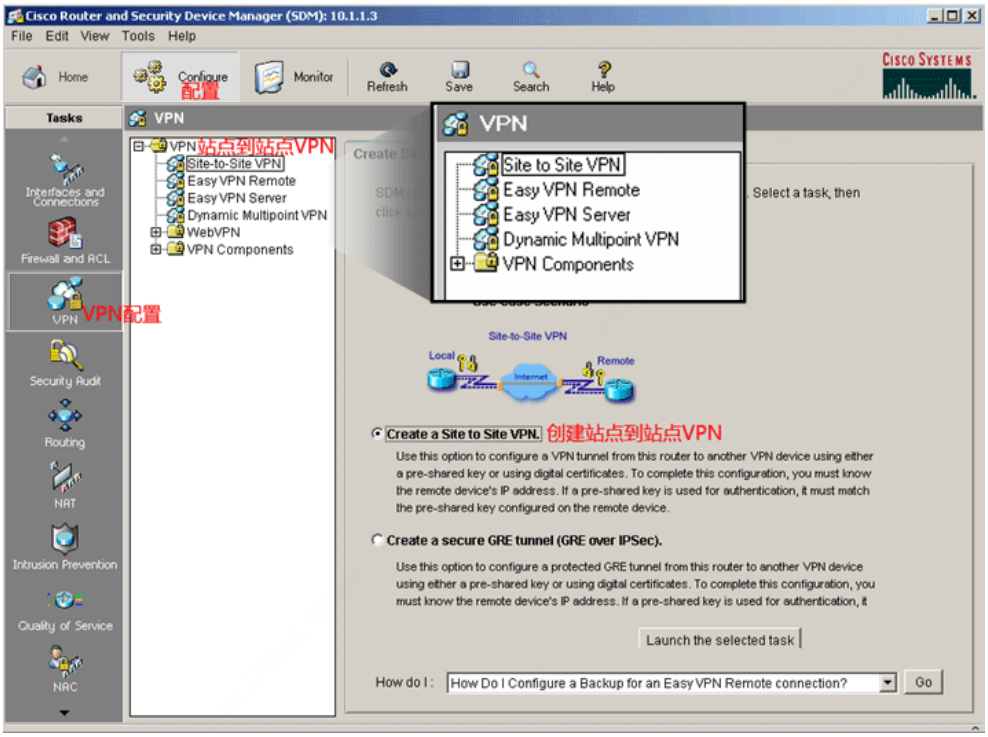
4、另外，为了避免SDM不能正常工作，需要对安装SDM的PC的活动内容进行启用。启用的方法是**打开 IE 浏览器，选择“工具”菜单项，继续选择“Internet 选项”， 在弹出的对话框中，选择“高级”选项卡，找到下图选项并打勾。中文是：“允许活动内容在我的计算机上的文件中运行”。**



5、启动SDM，并且填写需要管理的设备IP地址，并单击Launch按钮，如下图显示：

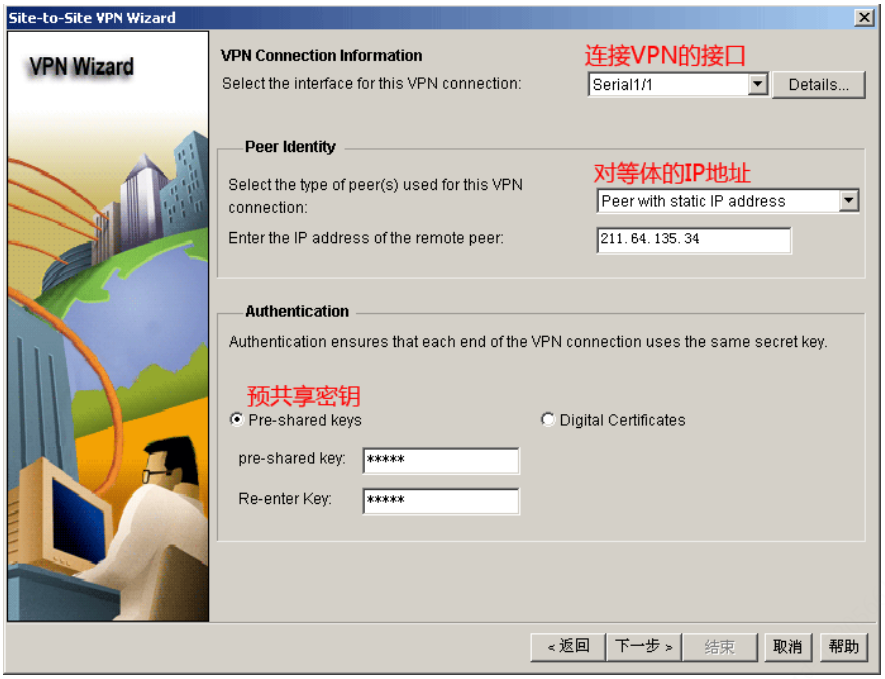


6、然后在 SDM 的界面中，选择“Configure”，继续选择“VPN”，然后选择“Site-to-Site VPN”，选择“Create a Site to Site VPN”，点击“Launch the selected task”。如下面所示：

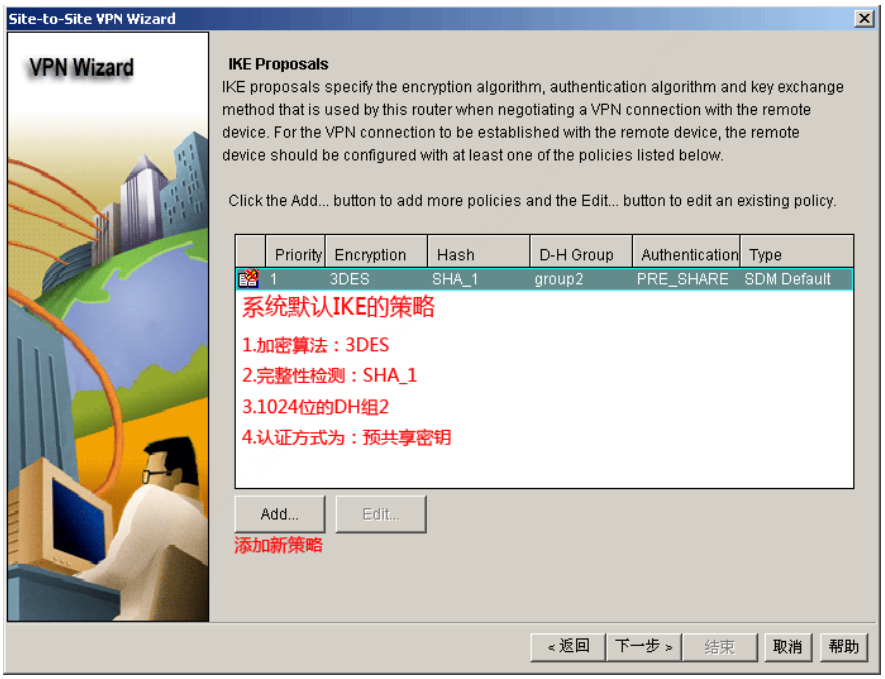


7、在新弹出的 Site-to-Site Wizard 对话框中，选择“Step by step wizard”，点击下一步。以便于清晰了解配置的全过程。

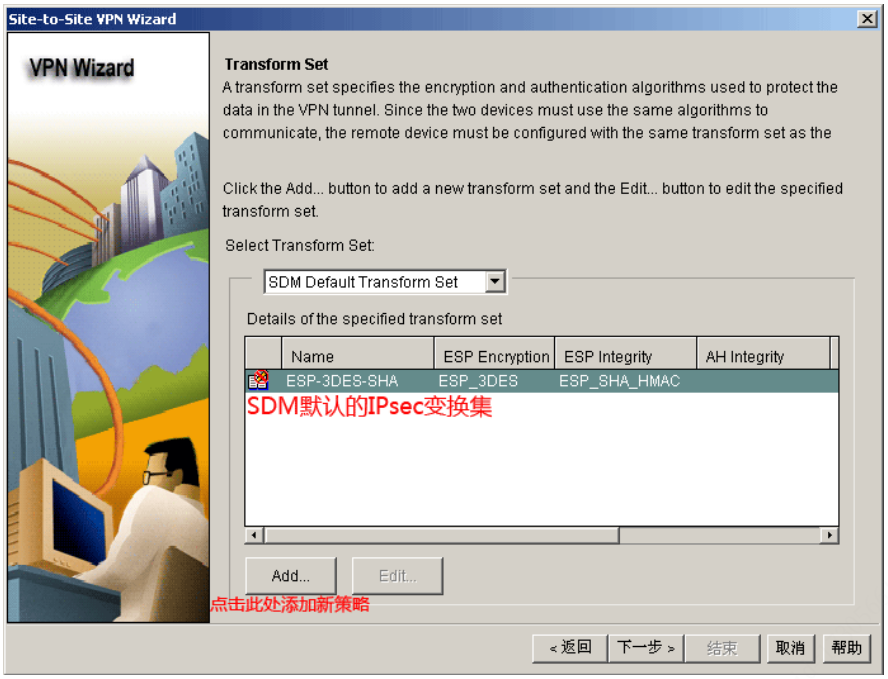
8、选择建立 VPN 的接口，配置对等体的 IP，选择认证类型。本实验选择了预共享密钥作为认证方式，因此还需要配置预共享的密钥。如下图所示：



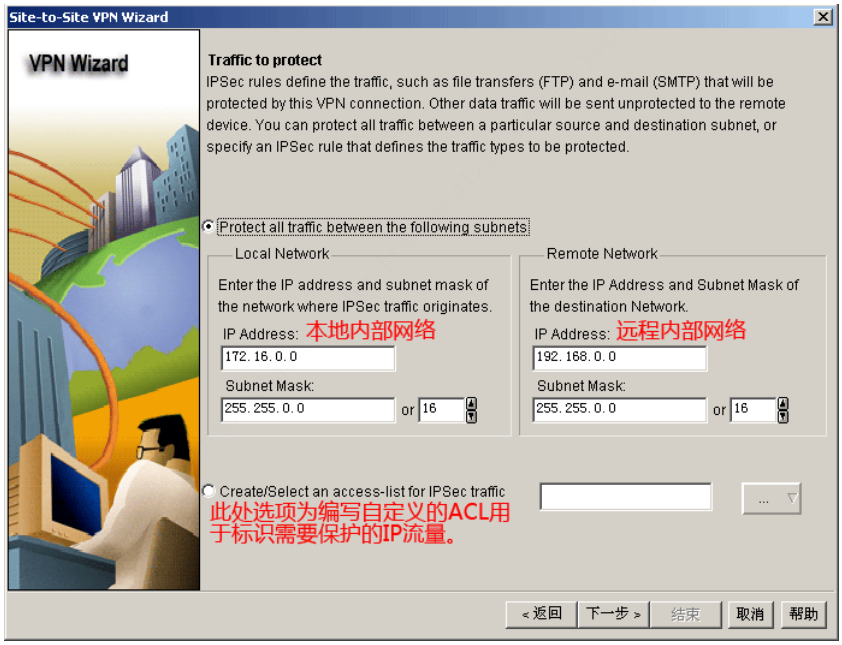
9、选择 IKE 的策略，也可以添加新策略，本实验使用默认策略：如下图所示：



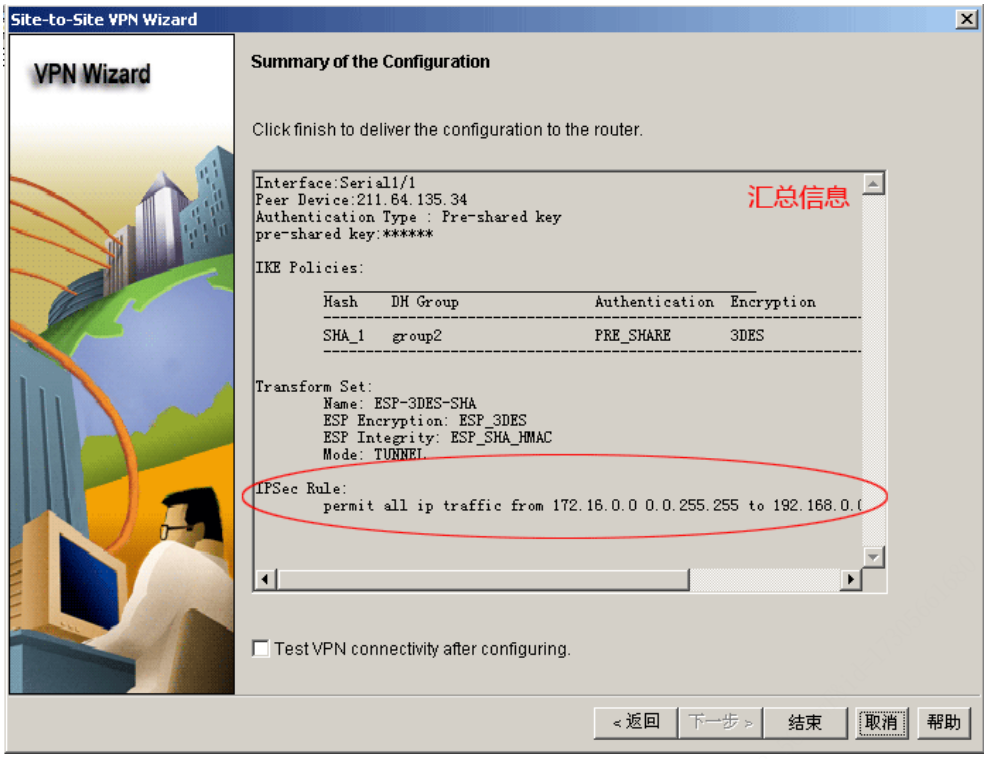
10、选择 IPsec 的变换集，本实验选择默认，也可能添加新策略，如下图所示：



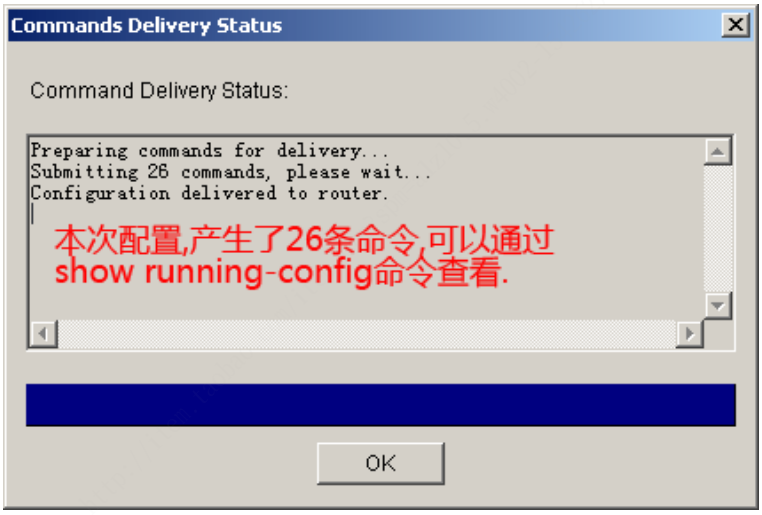
11、配置需要被加密保护的 IP 流量，也可以编写自定义的 ACL 进行定义。如下图所示：



12、查看配置汇总信息，如下图所示：



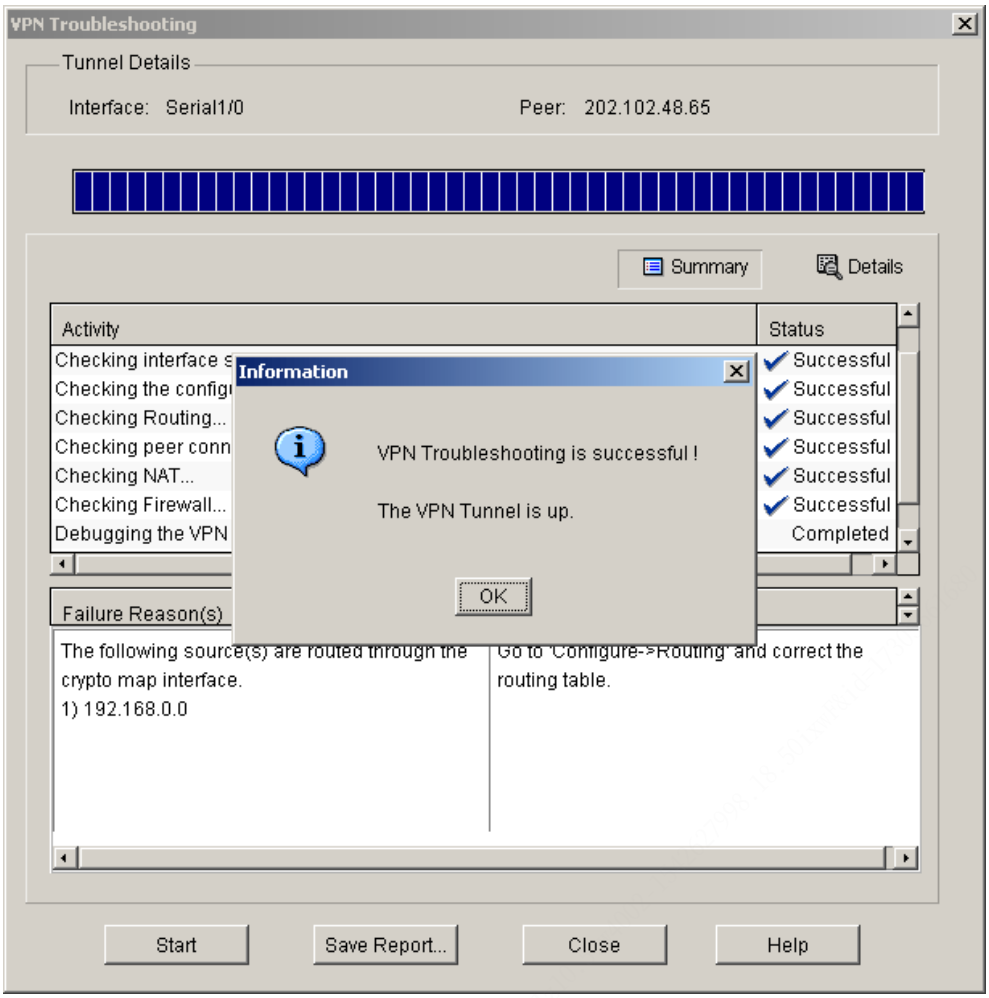
13、点击结束按钮，将生成的命令写入到 R1 路由器，如下图所示：



14、完成配置后，可以在 R1 路由器使用 show running-config 命令查看 SDM 生成的配置命令。

14、采用相同的配置步骤完成 R3 的配置，此处不再列出。

15、在 SDM 中选择 R1 或 R2 路由器测试隧道，如下图所示：



16、在 R1 或 R3 上使用扩展 ping 命令测试隧道：

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/132/188 ms
R1#
```

17、具体调试信息和其它状态查看，请参阅实验：Configuring IPsec Site-to-Site With Preshare-Key。

18、实验完成。

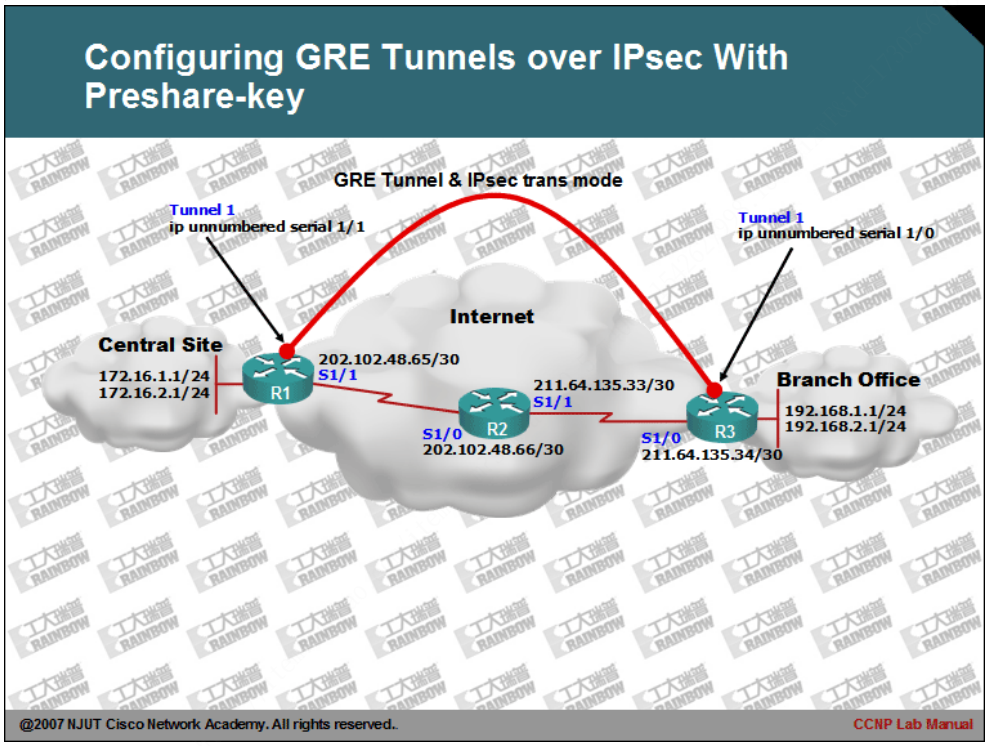
CCNP Lab Manual

Lab 63. Configuring GRE Tunnels over IPsec With Preshare-key

实验目的：

1、掌握基于预共享密钥的 IPsec 传输模式和 GRE 隧道配置方法。
2、通过 GRE 的隧道解决了 IPsec 仅支持 IP 协议和单播的特性。
3、IPsec 的隧道模式会破坏 GRE 的报头，因此必须配置为传输模式。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、在 R1 和 R3 上配置静态路由。确保 Internet 网络骨干可以相互通信。

```
R1(config)#ip route 0.0.0.0 0.0.0.0 202.102.48.66
```

```
R3(config)#ip route 0.0.0.0 0.0.0.0 211.64.135.33
```

3、在 R1 和 R3 路由器上配置 GRE 隧道。

```
R1(config)#interface tunnel 1
R1(config-if)#ip unnumbered serial 1/1
R1(config-if)#tunnel destination 211.64.135.34
R1(config-if)#tunnel source serial 1/1
R1(config-if)#no shutdown
R1(config-if)#exit
```

批注 [stanley703]：配置隧道的 IP 地址，借用物理接口 s1/0 的 IP。
这样做的目的，是避免 ISAKMP 在协商 SA 时，其预共享密钥匹配的问题。
如果配置单独的 IP 地址，则在进行预共享密钥匹配时，对等体的 IP 会使用其物理接口，而不隧道接口的 IP。

```
R3(config)#interface tunnel 1
R3(config-if)# ip unnumbered serial 1/0
R3(config-if)#tunnel source serial 1/0
R3(config-if)#tunnel destination 202.102.48.65
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

批注 [stanley704]：指定隧道目标。

批注 [stanley705]：指定隧道源。

4、查看 R1 或是 R3 的隧道接口状态。

```
R1#show inter tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Serial1/1 (202.102.48.65)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 202.102.48.65 (Serial1/1), destination 211.64.135.34
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
.....
```

5、在 R1 和 R3 上配置路由，确保 R1 和 R3 可以通过隧道 PING 通对方的回环接口。

```
R1(config)#ip route 192.168.0.0 255.255.0.0 tunnel 1
```

批注 [stanley706]：配置 R1 到达 192.168.0.0/16 网络其下跳为隧道的对等体 IP。

```
R3(config)#ip route 172.16.0.0 255.255.0.0 tunnel 1
```

6、在 R1 或是 R3 上使用 PING 命令，检测是否可以 PING 对方的回环接口。

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/40/60 ms
R1#
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/95/132 ms
R1#
```

7、在 R1 上配置 IPsec 的传输模式。

```
R1(config)#crypto isakmp enable
R1(config)#
R1(config)#crypto isakmp key 0 ciscokey address 211.64.135.34
R1(config)#
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 1
R1(config-isakmp)#exit
R1(config)#
R1(config)#crypto ipsec transform-set my_trans esp-des
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#
R1(config)#access-list 100 permit gre host 202.102.48.65 host 211.64.135.34
R1(config)#
R1(config)#crypto map gre_to_R3 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 211.64.135.34
R1(config-crypto-map)#set transform-set my_trans
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
```

批注 [stanley707]: 配置预共享密钥。

批注 [stanley708]: 配置 IPsec 的变换集。

批注 [stanley709]: 指定 IPsec 的工作模式为传输模式。

批注 [stanley710]: 针对 GRE 隧道的流量进行保护。

```
R1(config)#
R1(config)#interface s1/1
R1(config-if)#crypto map gre_to_R3
R1(config-if)#exit
```

```
R3(config)#crypto isakmp enable
R3(config)#
R3(config)#crypto isakmp key 0 ciscokey address 202.102.48.65
R3(config)#
R3(config)#crypto isakmp policy 1
R3(config-isakmp)#hash md5
R3(config-isakmp)#encryption des
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 1
R3(config-isakmp)#exit
R3(config)#
R3(config)#crypto ipsec transform-set my_trans esp-des
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit
R3(config)#
R3(config)# access-list 100 permit gre host 211.64.135.34 host 202.102.48.65
R3(config)#
R3(config)#crypto map gre_to_R1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 202.102.48.65
R3(config-crypto-map)#set transform-set my_trans
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#
R3(config)#interface s1/0
R3(config-if)#crypto map gre_to_R1
R3(config-if)#exit
R3(config)#
```

8、开启对 ISAKMP 和 Ipsec 的协商的调试。

```
R1#debug crypto isakmp
R1#debug crypto ipsec
```

```
R3#debug crypto isakmp
R3#debug crypto ipsec
```

具体的协商过程请大家参阅实验：Configuring IPsec Site-to-Site With Preshare-Key 的 debug 信息解释。

9、在 R1 或 R3 路由器上使用扩展 ping 命令，触发 IPsec 的协商。

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
..!!!
Success rate is 60 percent (2/5), round-trip min/avg/max = 36/64/112 ms
R1#
```

批注 [stanley711]：出现两丢包现象，是因为此时 IPsec 在尚未协商成功。后面！号表示协商已成功。

10、查看 ISAKMP 的安全关联，确认 IKE 阶段 1 的协商成功。

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
211.64.135.34   202.102.48.65   QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

11、查看 IKE 阶段 2 的安全关联。

```
R1#show crypto ipsec sa

interface: Serial1/1
    Crypto map tag: gre_to_R3, local addr 202.102.48.65

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (202.102.48.65/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (211.64.135.34/255.255.255.255/47/0)
   current_peer 211.64.135.34 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
```

```
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 202.102.48.65, remote crypto endpt.: 211.64.135.34
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/1
     current outbound spi: 0x1175F98F(292944271)

.....

     inbound esp sas:
      spi: 0xCB8175ED(3414259181)
        transform: esp-des ,
        in use settings ={Transport, }
        conn id: 1, flow_id: 1, crypto map: gre_to_R3
        sa timing: remaining key lifetime (k/sec): (4527485/3084)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE

     outbound esp sas:
      spi: 0x1175F98F(292944271)
        transform: esp-des ,
        in use settings ={Transport, }
        conn id: 2, flow_id: 2, crypto map: gre_to_R3
        sa timing: remaining key lifetime (k/sec): (4527483/3084)
        IV size: 8 bytes
        replay detection support: N
        Status: ACTIVE

.....

R1#
```

批注 [stanley712]： 描述了，有多个数据包被加解密。

其对于实验有重要意义。每次发送 PING 数据包后，观察此处，会发现数字会增加。说明数据确实是被 IPsec 所保护。

批注 [stanley713]： 此处指出 IPsec 目前工作于传输模式。

批注 [stanley714]： 而且其 SA 状态为 ACTIVE 状态。

12、查看会话信息。

```
R1#show crypto session
Crypto session current status

Interface: Serial1/1
Session status: UP-ACTIVE
Peer: 211.64.135.34 port 500
  IKE SA: local 202.102.48.65/500 remote 211.64.135.34/500 Active
```

批注 [stanley715]： 创建 IPsec 的会话接口。

批注 [stanley716]： 对等体的 IP 及所使用的 UDP 的端口号。

```
  IPSEC FLOW: permit 47 host 202.102.48.65 host 211.64.135.34
        Active SAs: 2, origin: crypto map


R1#
```

19、实验完成。

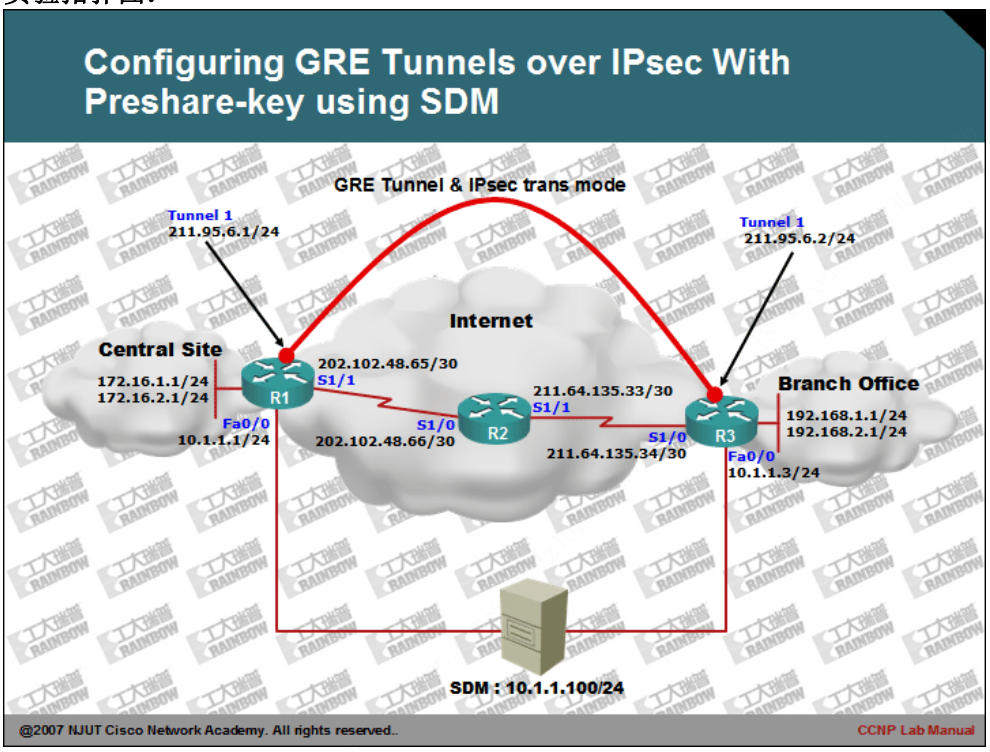
CCNP Lab Manual

Lab 64. Configuring GRE Tunnels over IPsec using SDM

实验目的：

1、掌握如何利用 SDM 来配置基于 GRE 的 IPsec 的 Site-to-Site VPN.

实验拓扑图：



实验步骤及要求：

1、首先在一台 PC 上安装 Cisco SDM 软件,并且需要安装 JAVA 环境。

2、配置各台路由器的 IP 地址，并且使用 ping 命令确认各路由器的直连口的互通性。其中 R1、R2 和 R3 的基本配置如下

```
R1(config)#interface loopback 0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip address 172.16.2.1 255.255.255.0 secondary
R1(config-if)#exit
R1(config)#interface serial 1/1
R1(config-if)#ip address 202.102.48.65 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 202.102.48.66
R1(config)#
```

批注 [stanley717]：配置此接口用于与 SDM 连接。

```
R2(config)#interface serial 1/0
R2(config-if)#ip address 202.102.48.66 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config-if)#
R2(config)#interface serial 1/1
R2(config-if)#ip address 211.64.135.33 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

```
R3(config)#interface loopback 0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#ip address 192.168.2.1 255.255.255.0 secondary
R3(config-if)#exit
R3(config)#interface serial 1/0
R3(config-if)#ip address 211.64.135.34 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip address 10.1.1.3 255.255.255.0
```

批注 [stanley718]：此地址用于连接到 SDM 服务器。

```
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
R3(config)#ip route 0.0.0.0 0.0.0.0 211.64.135.33
R3(config)#
```

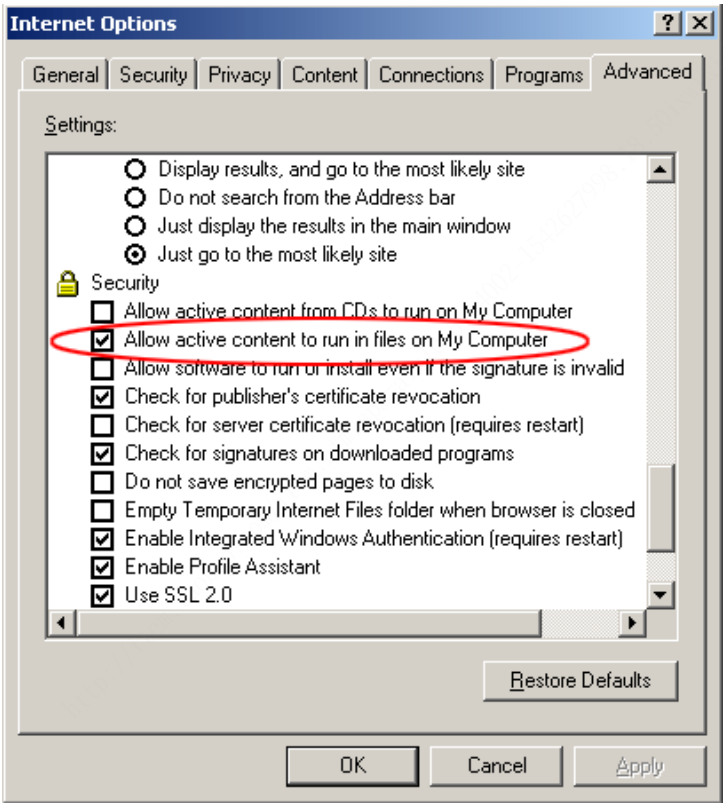
3、为了能够让SDM连接到R1和R3路由器，因此需要在R1和R3上启用http server服务，配置如下：

```
R1(config)#ip http server
```

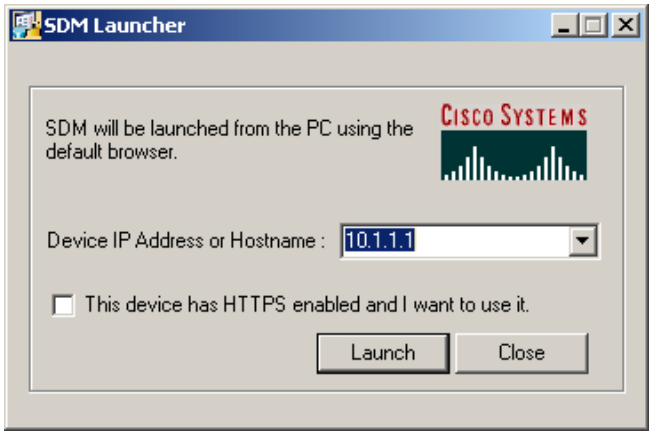
批注 [stanley719]: 启用ip http server服务。

```
R3(config)#ip http server
```

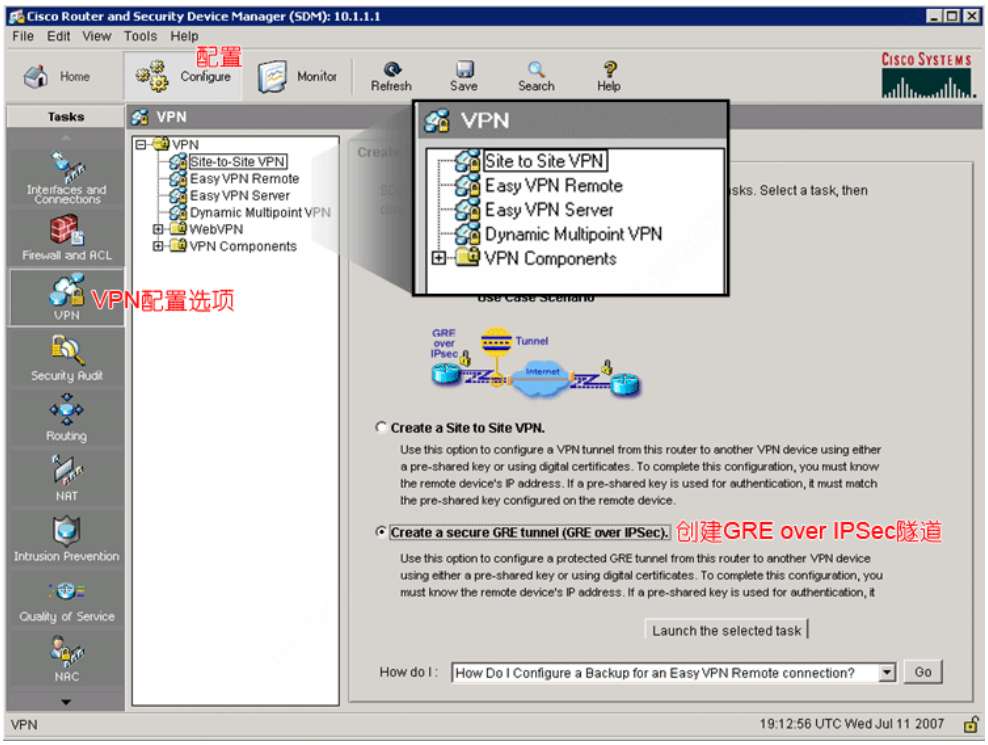
4、另外，为了避免SDM不能正常工作，需要对安装SDM的PC的活动内容进行启用。启用的方法是**打开 IE 浏览器，选择“工具”菜单项，继续选择“Internet选项”， 在弹出的对话框中，选择“高级”选项卡，找到下图选项并打勾。中文是：“允许活动内容在我的计算机上的文件中运行”。**



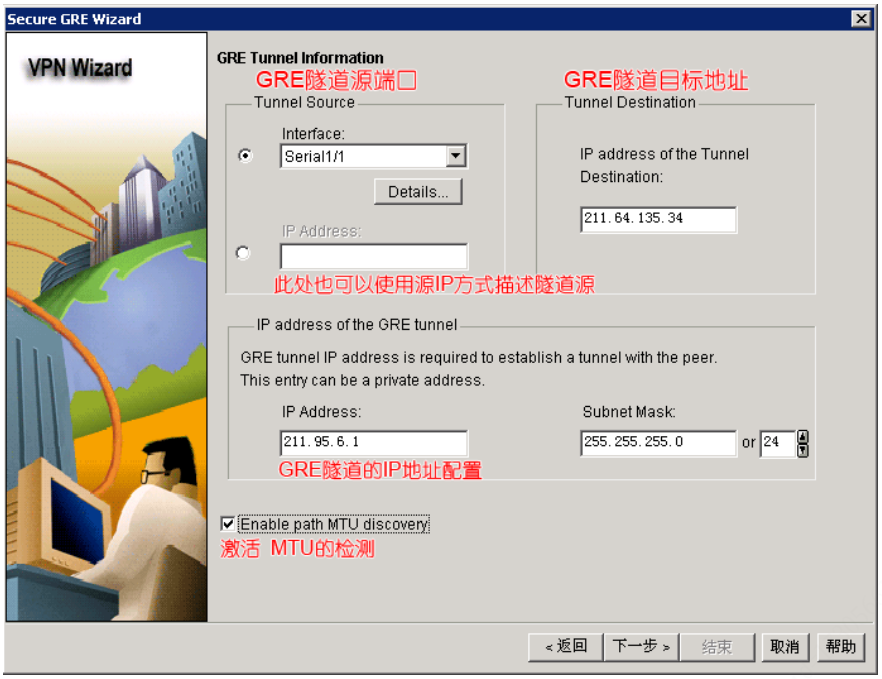
5、启动SDM并且填写需要管理设备IP地址，并单击Launch按钮，如下图显示：



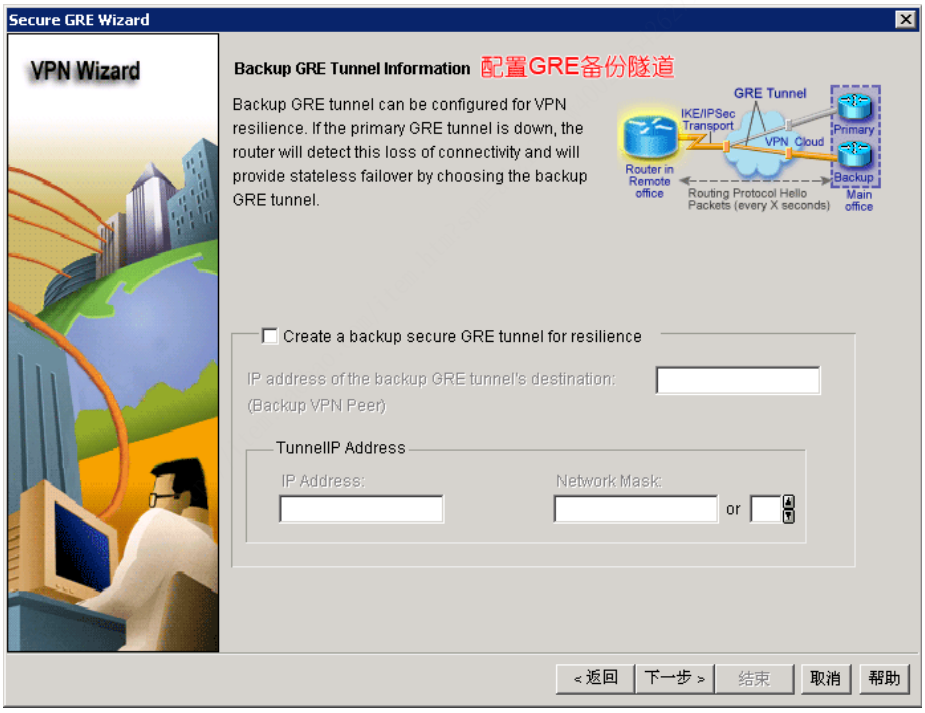
6、然后在 SDM 的界面中，选择“Configure”，继续选择“VPN”，然后选择“Site-to-Site VPN”，选择“Create a Site to Site VPN”，点击“Launch the selected task”。如下面所示：



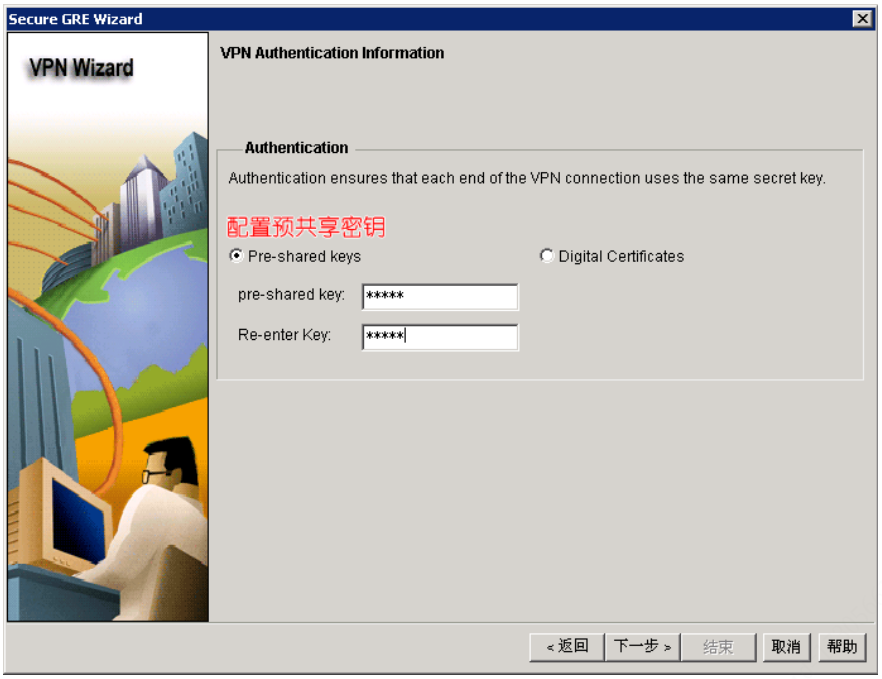
7、配置 GRE 隧道参数，如下图所示：



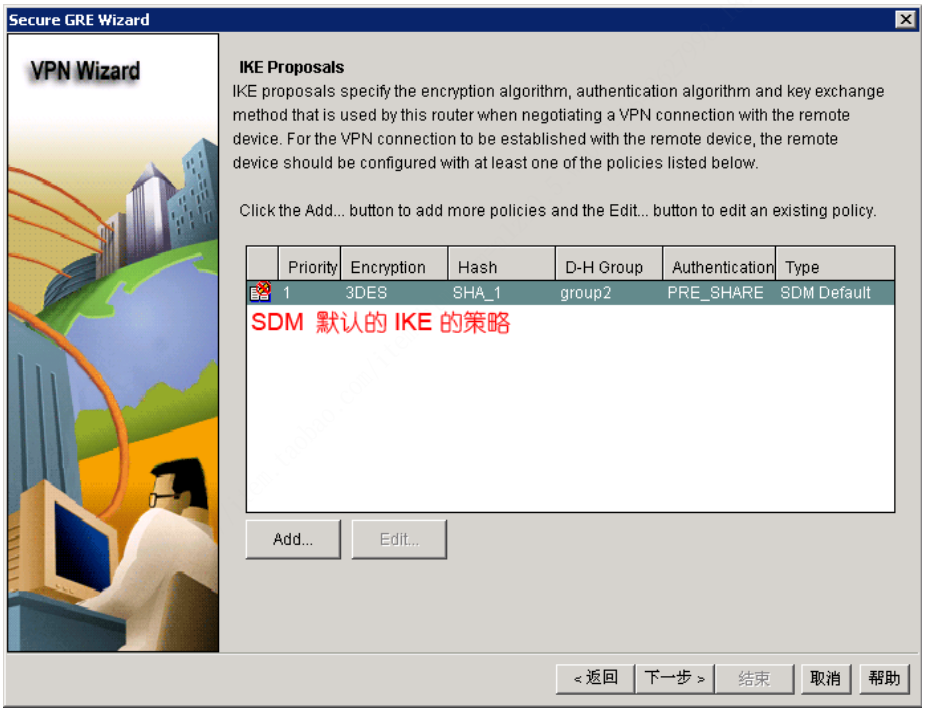
8、配置 GRE 的备份隧道，由于本实验不包含备份隧道，因此，此处直接点击下一步，如下图：



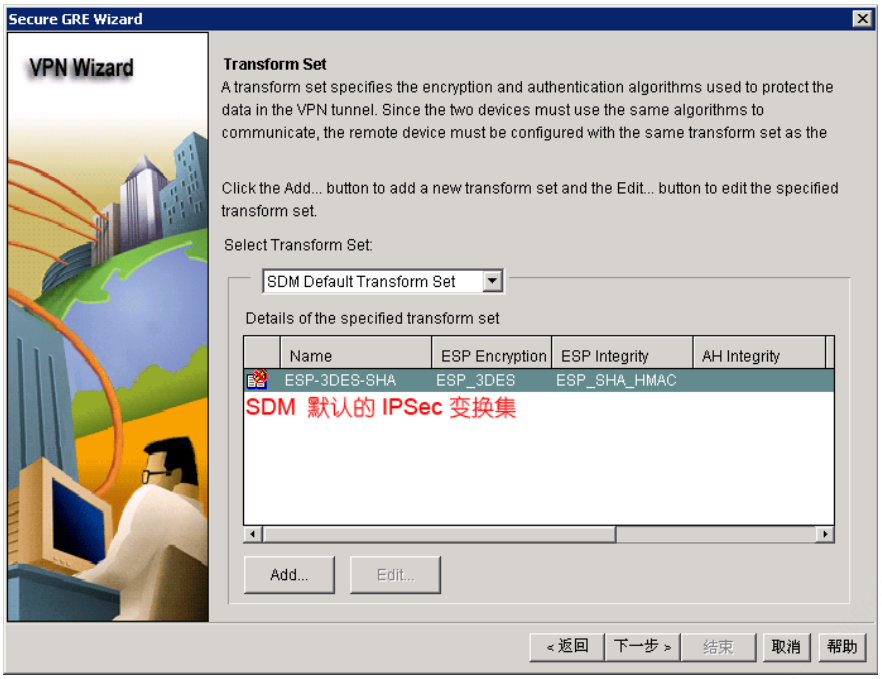
9、配置预共享密钥，如下图所示：



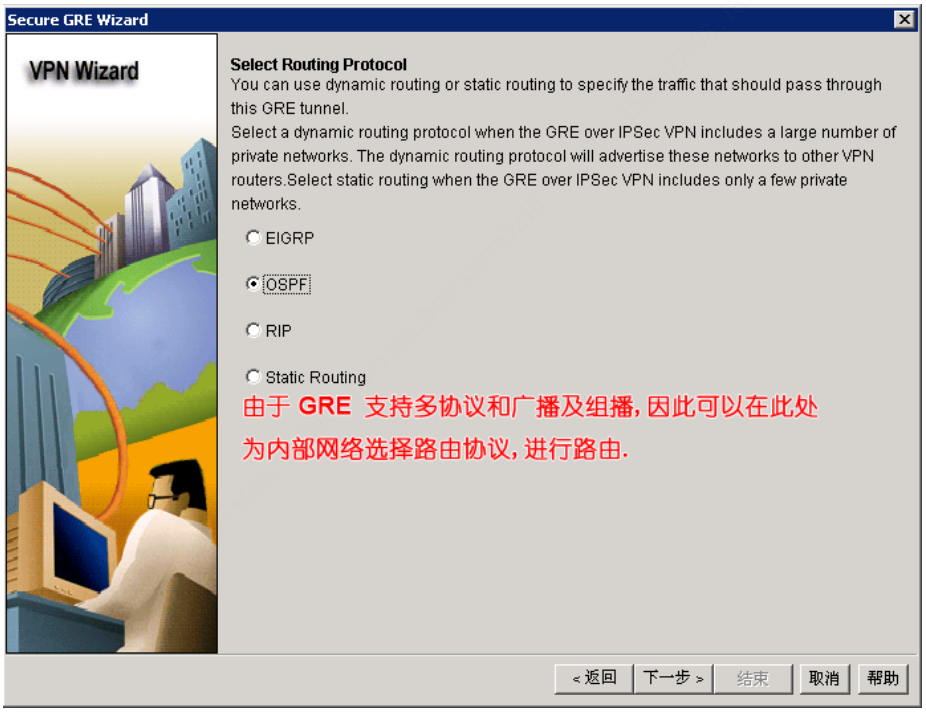
10、配置 ISAKMP 策略，如下所示：



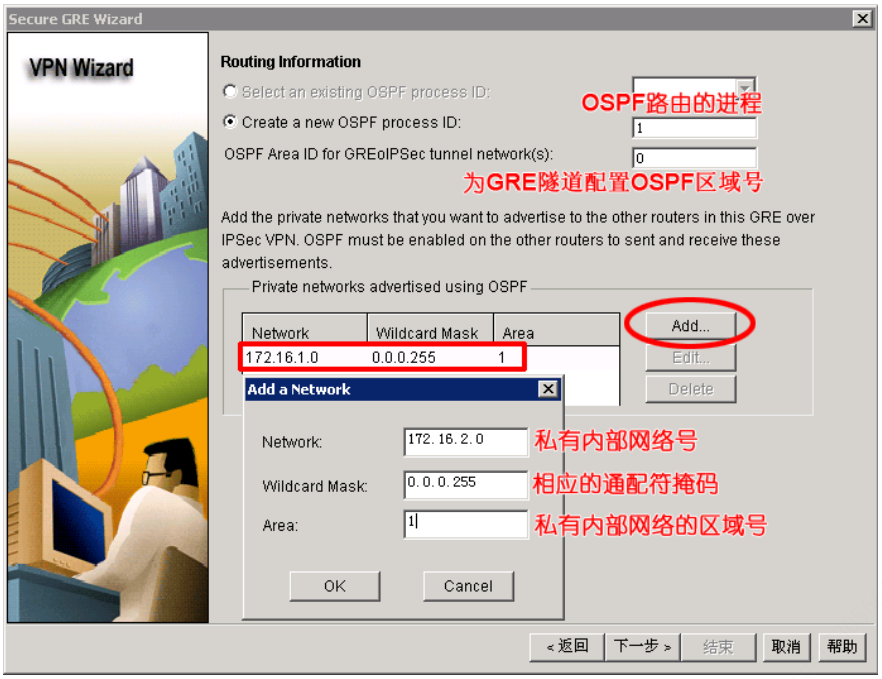
11、配置 IPSec 的变换集，如下图所示：



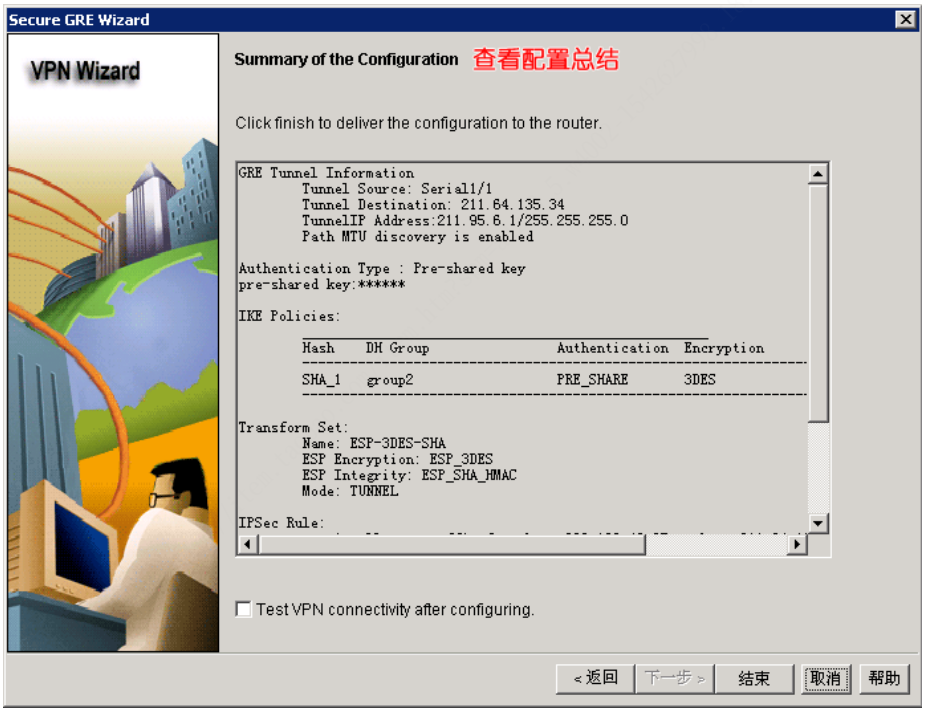
12、为 R1 与 R3 的私有网络，选择路由协议，本实验选择 OSPF，如下图所示：



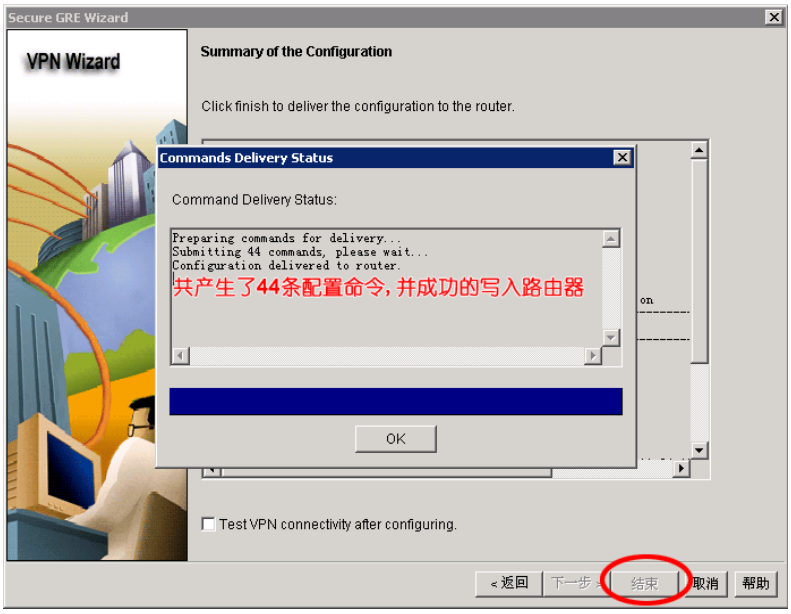
13、配置选择的 OSPF 路由协议，如下图所示（请结合拓扑阅读 OSPF 配置）：



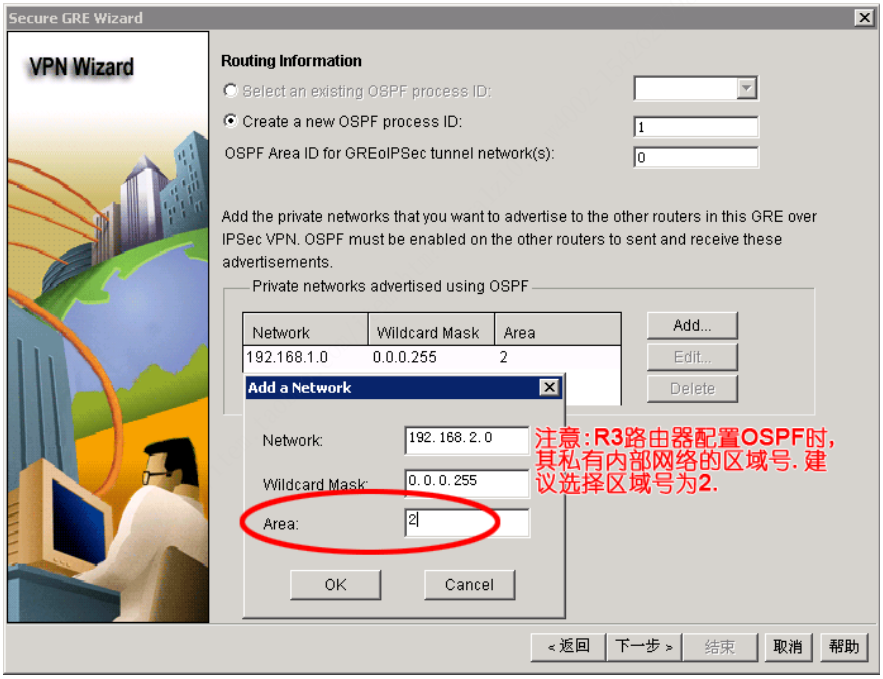
14、查看配置总结信息，如下图所示：



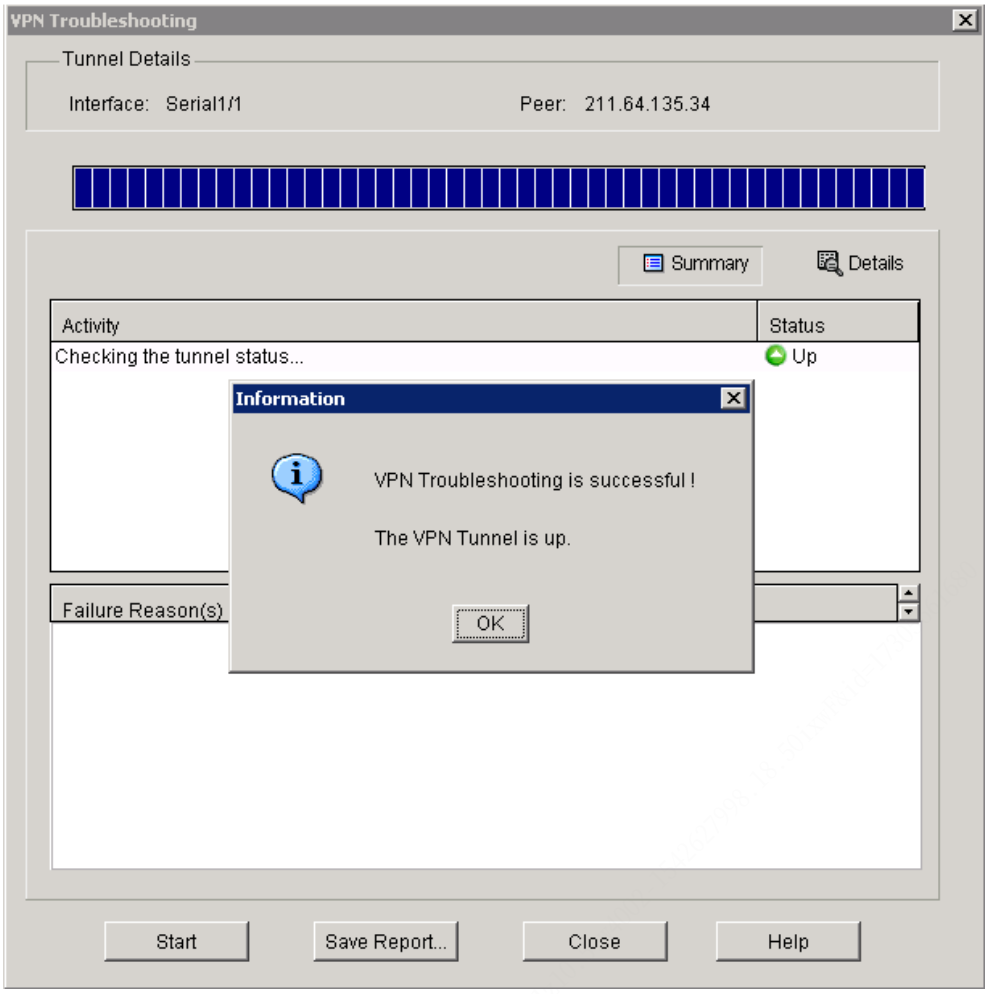
15、点击结束，SDM 将生成的配置，写入到 R1 路由器，如下图所示：



16、点击 OK 按键，结束对 R1 的配置，采用相同的配置方法，对 R3 进行配置，需要注意的是在配置 R3 路由器的 OSPF 配置时，需要为 R3 路由器的私有内部网络选择不同的区域号，以避免产生区域被分隔的问题，如下图所示：



17、当完成配置后，可以在 R1 或 R3 的 SDM 的管理界面上，使用 SDM 的自带的测试功能，对隧道进行测试，如下图所示：



18、选择 R1 或 R3 路由器，使用 show running-config 查看 SDM 产生的配置命令：

```
R1#show running-config
.....
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key cisco address 211.64.135.34
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to211.64.135.34
 set peer 211.64.135.34
 set transform-set ESP-3DES-SHA
```

```
 match address 100
!
interface Tunnel0
 ip address 211.95.6.1 255.255.255.0
 ip mtu 1420
 ip ospf mtu-ignore
 tunnel source Serial1/1
 tunnel destination 211.64.135.34
 tunnel path-mtu-discovery
 crypto map SDM_CMAP_1
.....
R1#
```

19、查看 R1 的 OSPF 的邻居信息：

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.1       0   FULL/  -        00:00:39    211.95.6.2      Tunnel0
R1#
```

批注 [stanley720]：由 R3 路由器建立了邻居关系。

20、查看 R1 的路由表：

```
R1#show ip route

Gateway of last resort is 202.102.48.66 to network 0.0.0.0

     202.102.48.0/30 is subnetted, 1 subnets
C       202.102.48.64 is directly connected, Serial1/1
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback0
C       172.16.2.0 is directly connected, Loopback0
C    211.95.6.0/24 is directly connected, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
     192.168.1.0/32 is subnetted, 1 subnets
O IA    192.168.1.1 [110/11112] via 211.95.6.2, 00:07:03, Tunnel0
O IA 192.168.2.0/24 [110/11112] via 211.95.6.2, 00:07:03, Tunnel0
S*   0.0.0.0/0 [1/0] via 202.102.48.66
R1#
```

批注 [stanley721]：由于隧道的原因，OSPF 从邻居 R3 学习到的远程网络路由。

注意其下一跳的出口为隧道。

21、在 R1 和 R3 上分别使用 ping 命令测试网络：

```
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/102/128 ms
R1#
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/72/136 ms
R1#
```

```
R3#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/118/160 ms
R3#
R3#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/80/136 ms
R3#
```

22、实验完成。

CCNP Lab Manual

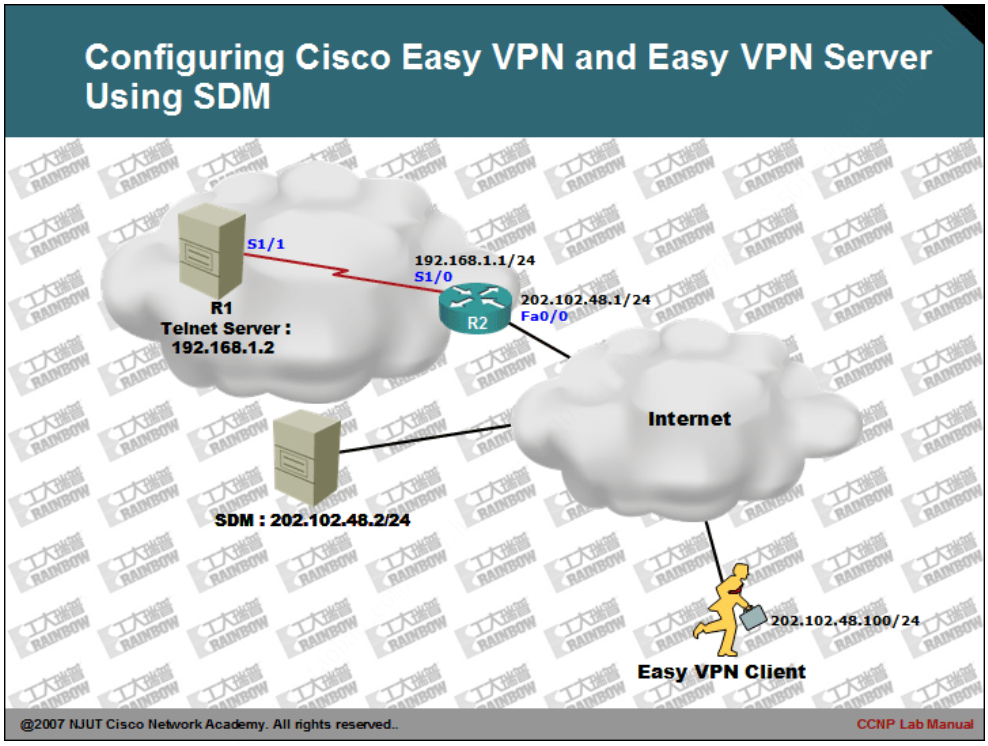
Lab 65. Configuring Cisco Easy VPN and Easy VPN Server Using SDM

实验目的：

1、掌握如何使用 SDM 配置 Easy VPN Server。

2、使用 Easy VPN Client 软件连接到 Easy VPN 服务器。

实验拓扑图：



实验步骤及要求：

1、将 R1 路由器配置为 Telnet 服务器，用于测试 Easy VPN 的客户端的连接，配置如下：

```
R1(config)#interface serial 1/1
R1(config-if)#ip address 192.168.1.2 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

批注 [stanley722]：配置默认路由指向 R2 路由器。

2、配置 R2 路由器基本配置，以接受 SDM 的配置：

```
R2(config)#interface serial 1/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#interface fastEthernet 0/0
R2(config-if)#ip address 202.102.48.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#aaa new-model
R2(config)#
R2(config)#aaa authentication login default local
R2(config)#
R2(config)#username wangyuan privilege 15 password cisco
R2(config)#
```

批注 [stanley723]：Easy VPN Server 需要 AAA 的支持。

批注 [stanley724]：防止由于控制台超时而无法连接路由器控制台，注意此配置与 Easy VPN 无关。

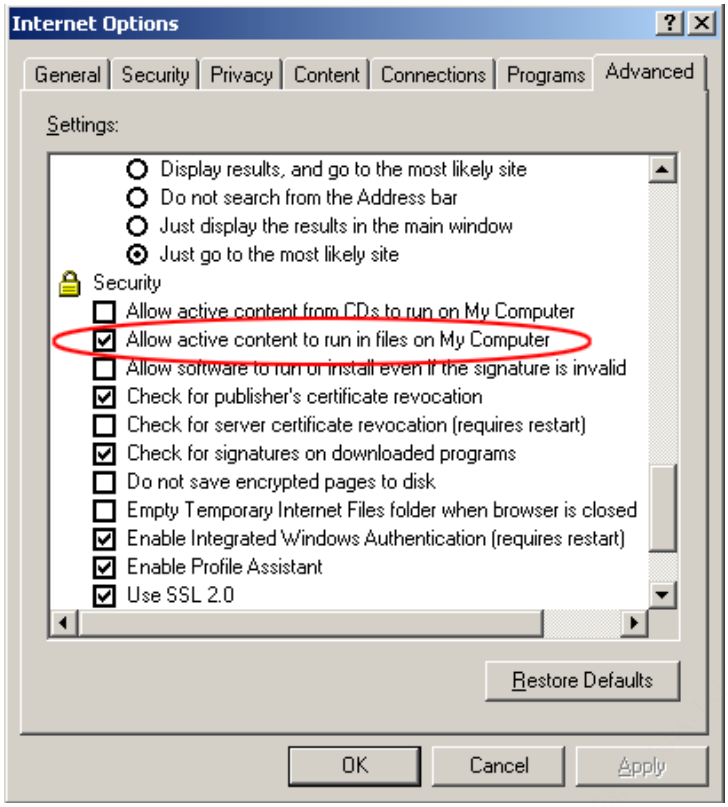
批注 [stanley725]：创建一个特权为 15 的帐号，用于本地路由器的登录。

3、为了能够让 SDM 连接到 R2 路由器，因此需要在 R2 上启用 http server 服务，配置如下：

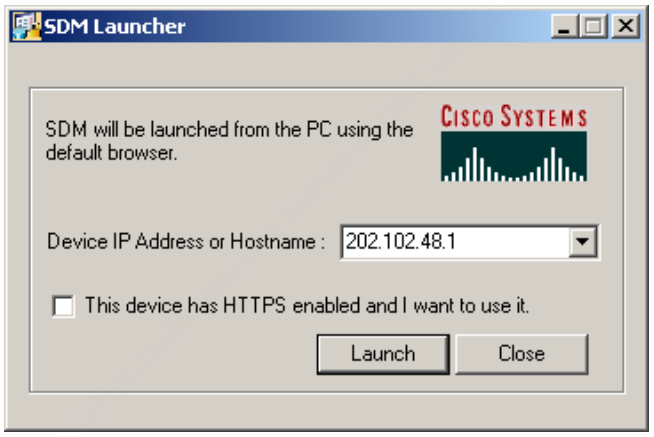
```
R2(config)#ip http server
```

批注 [stanley726]：启用 ip http server 服务。

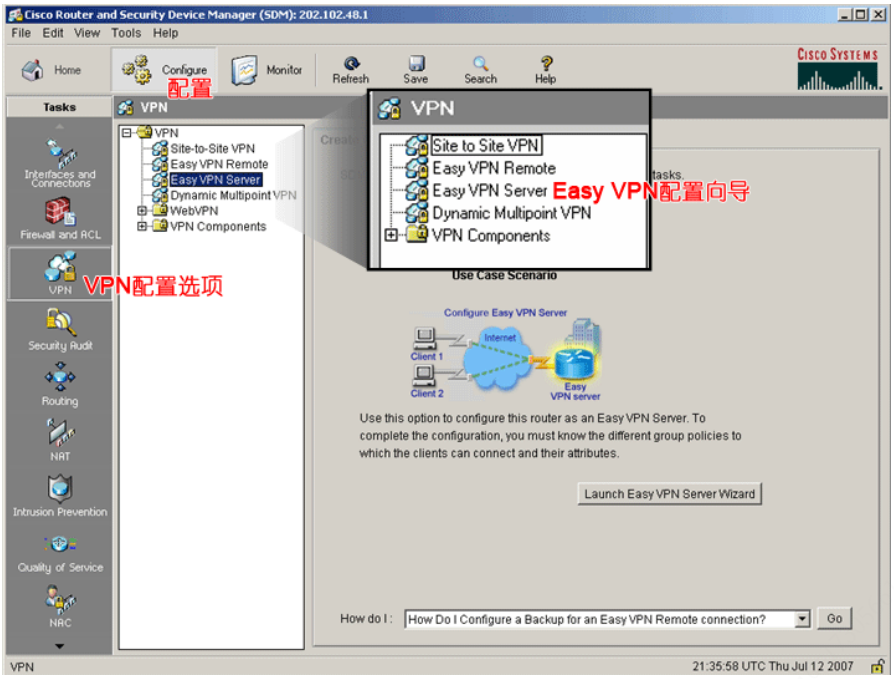
4、另外，为了避免 SDM 不能正常工作，需要对安装 SDM 的 PC 的活动内容进行启用。启用的方法是**打开 IE 浏览器，选择“工具”菜单项，继续选择“Internet 选项”， 在弹出的对话框中，选择“高级”选项卡，找到下图选项并打勾。中文是：“允许活动内容在我的计算机上的文件中运行”。**



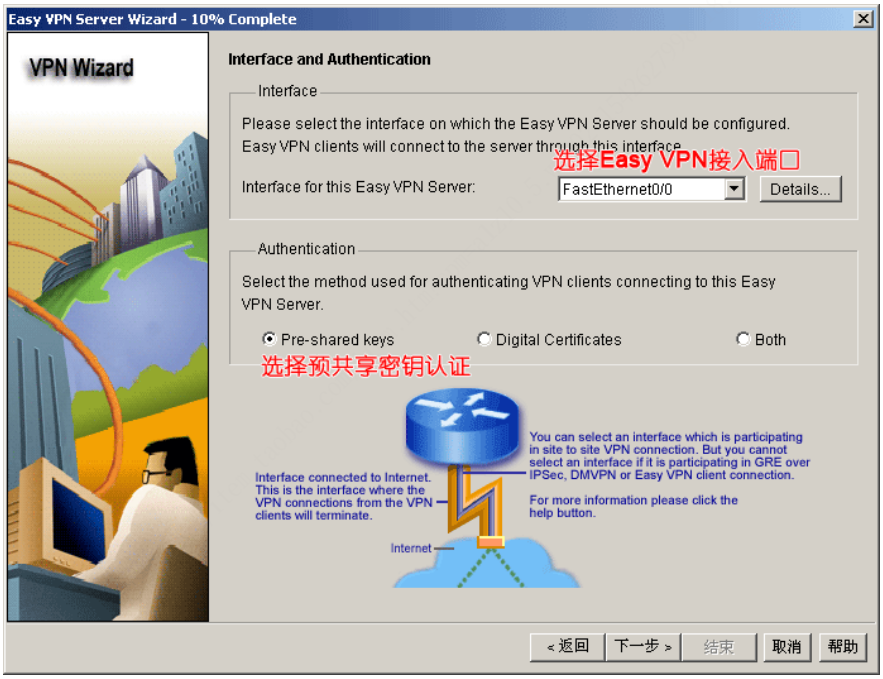
5、启动 SDM 并且填写需要管理设备 IP 地址，并单击 Launch 按钮，如下图显示：



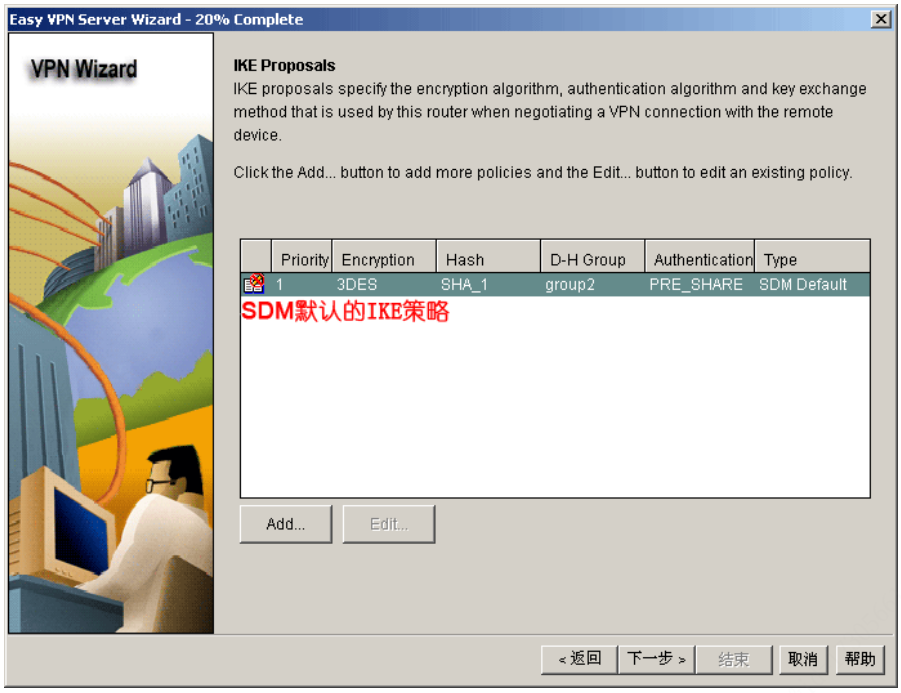
6、然后在 SDM 的界面中，选择“Configure”，继续选择“VPN”，然后选择“Site-to-Site VPN”，选择“Create a Site to Site VPN”，点击“Launch the selected task”。如下面所示：



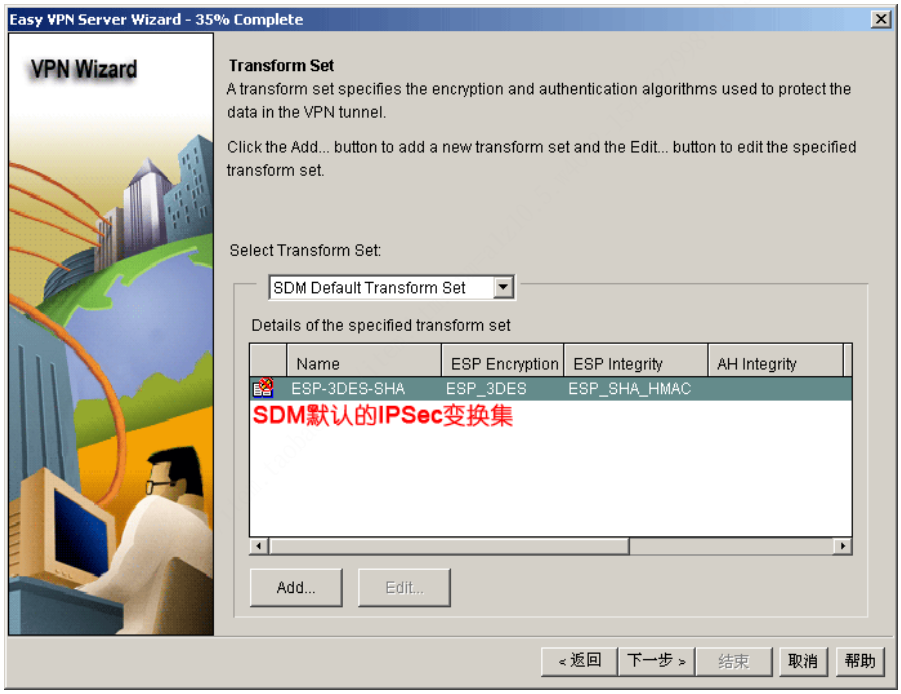
7、选择 Easy VPN Server 接入端口和认证方式：



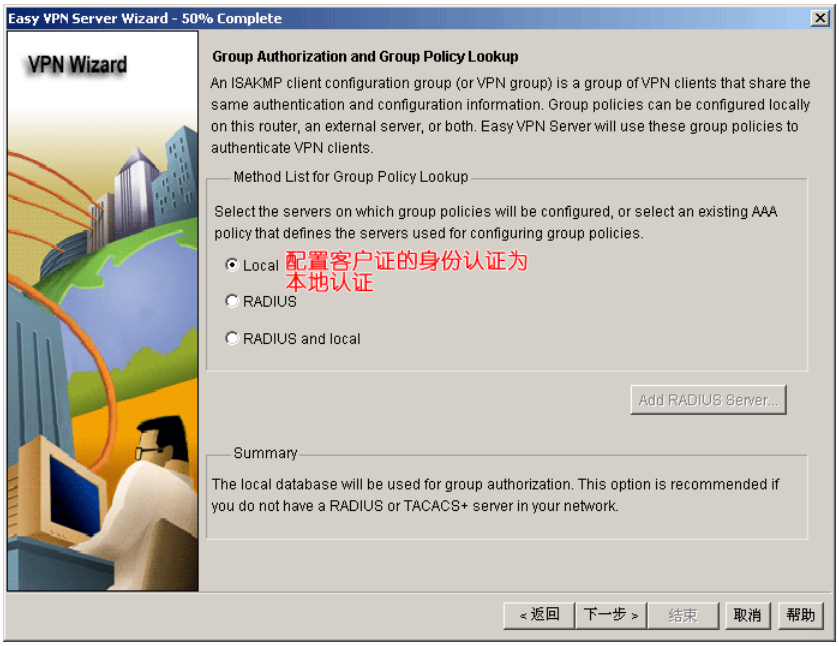
8、配置 IKE 策略：



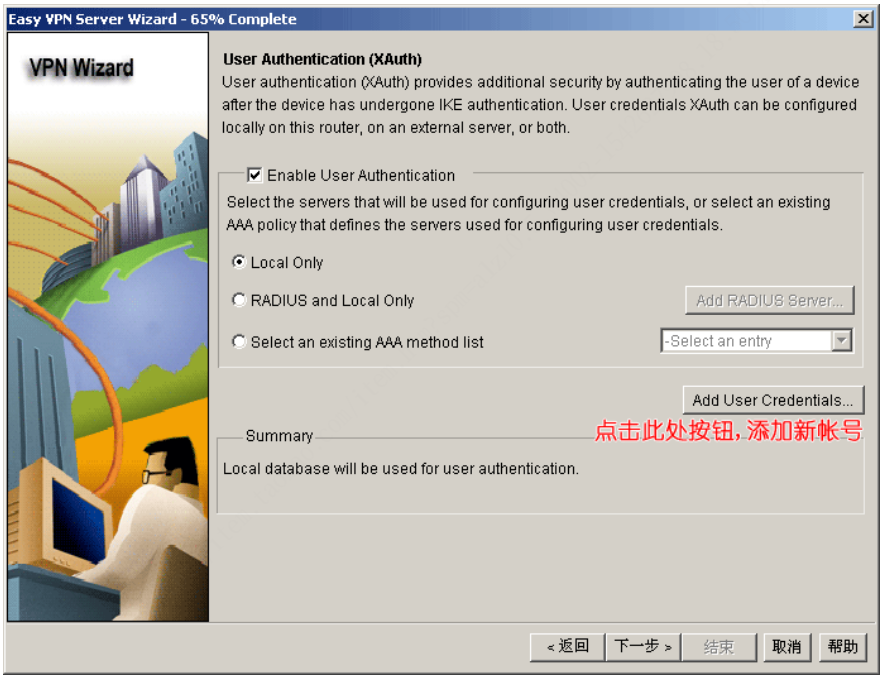
9、配置 IPSec 变换集，如下图所示：



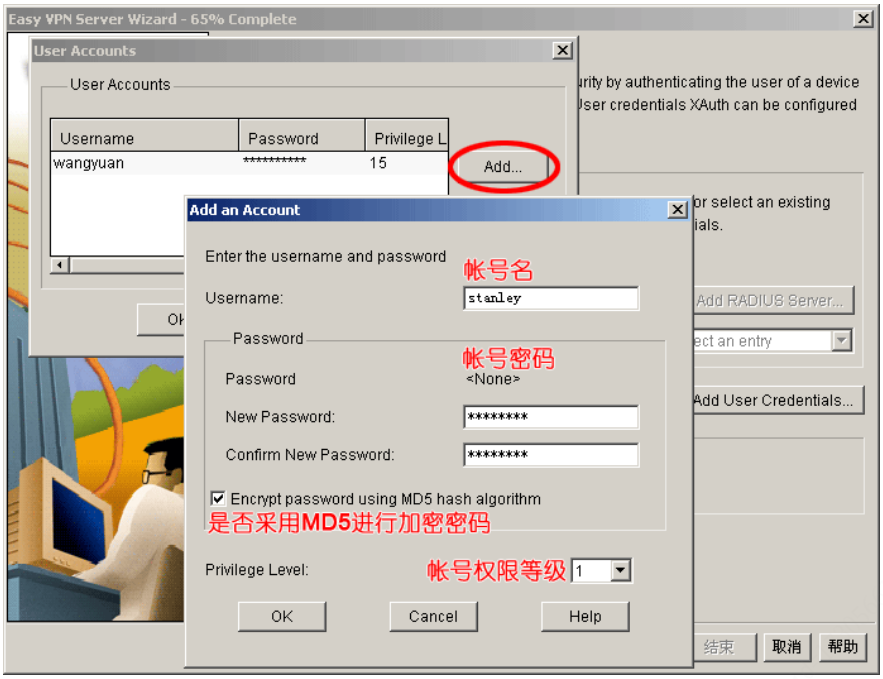
10、配置客户端的身份认证方式，为本地用户名密码数据库，也可以配置 ACS 服务器进行身份认证：



11、添加 Easy VPN 的用户帐号：

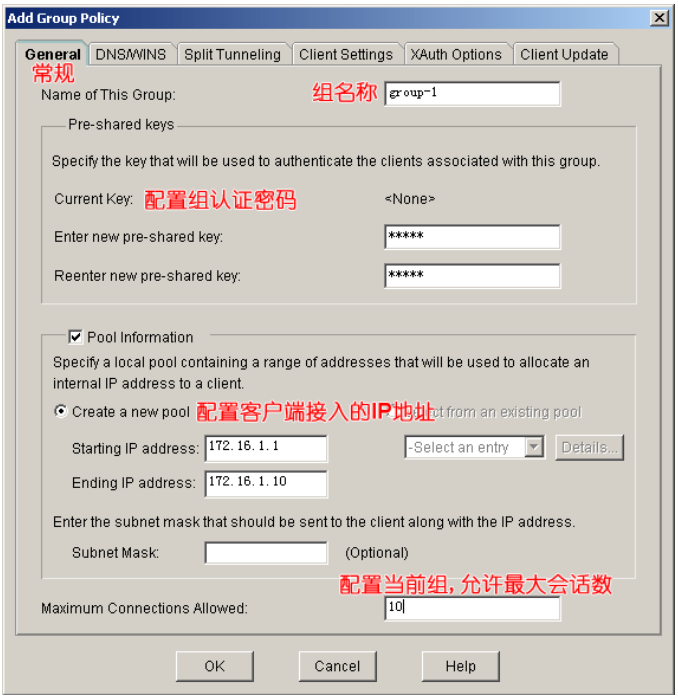


12、创建一个用于 VPN 客户端连接的帐号：

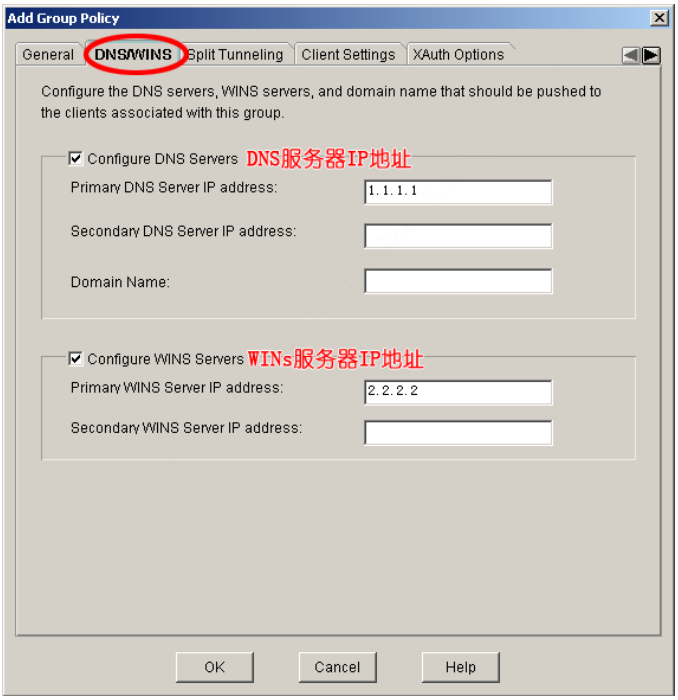


13、配置 Easy VPN 组策略，配置如下：

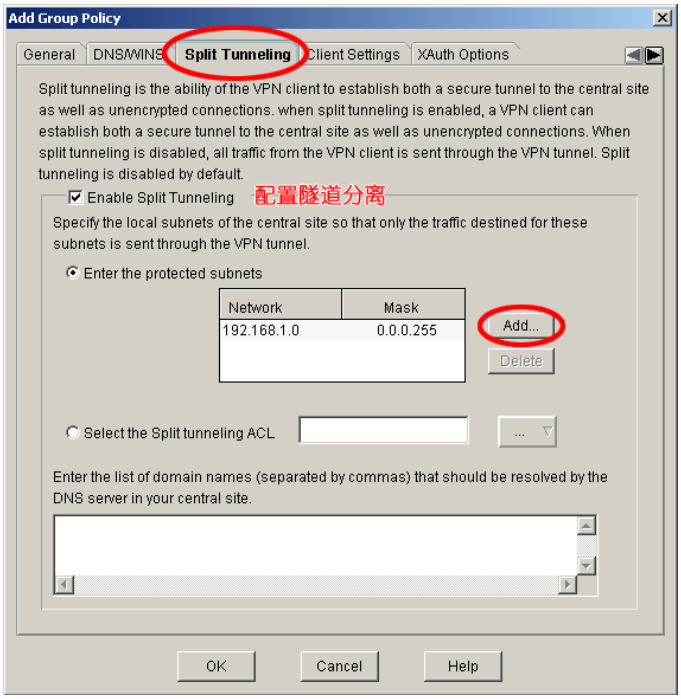
14、配置组名称、组最大会话数、认证密码以及客户端连接后的 IP 地址：



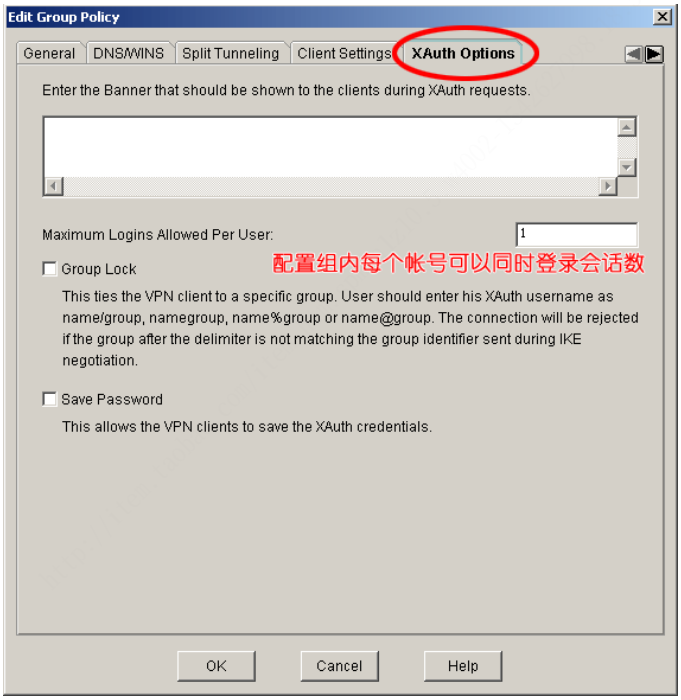
15、配置客户端的 DNS 以及 WINs 的服务器地址：



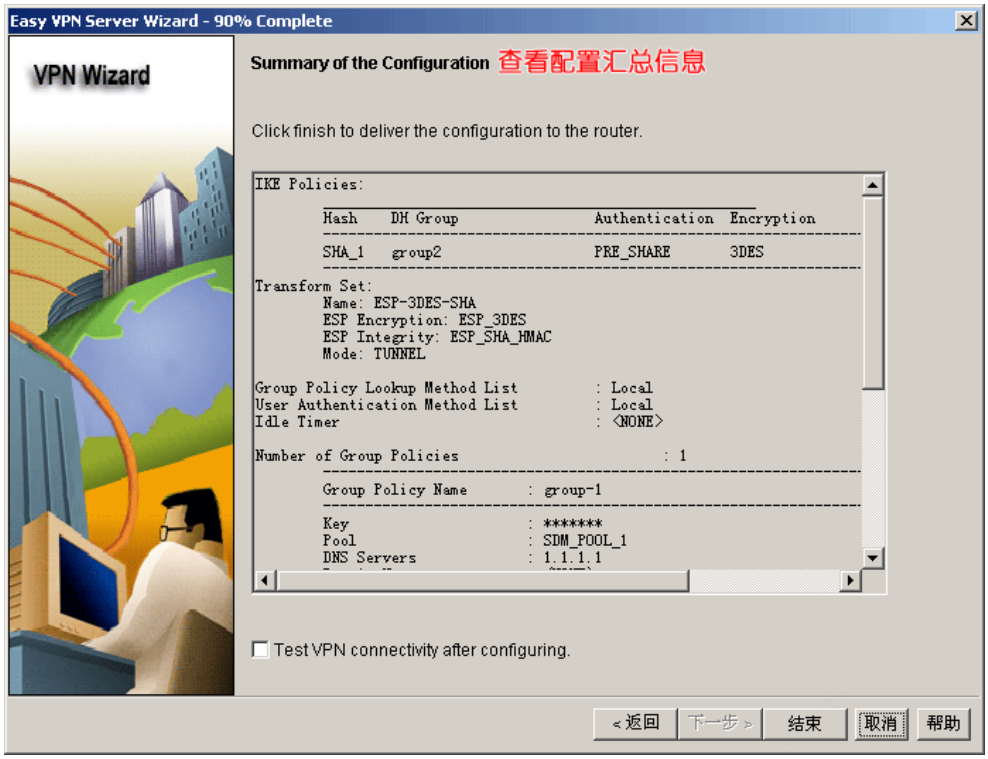
16、配置隧道分离：



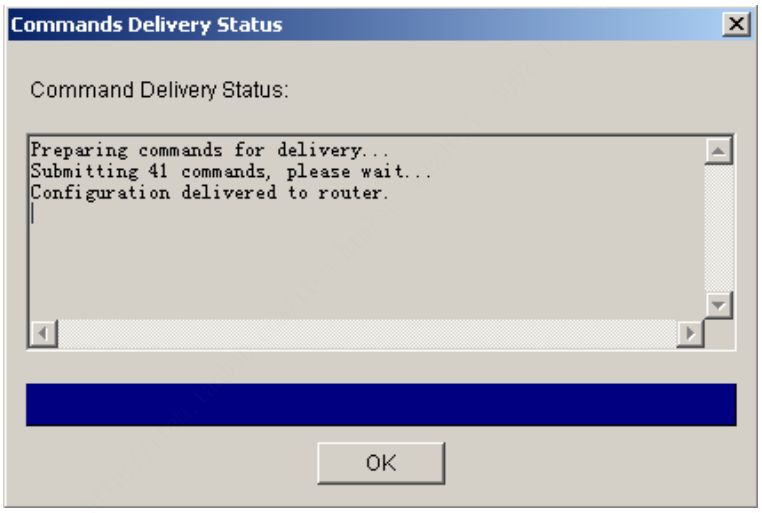
17、配置帐号策略，仅允许单点登录，同时还可以配置是否允许客户端保存密码：



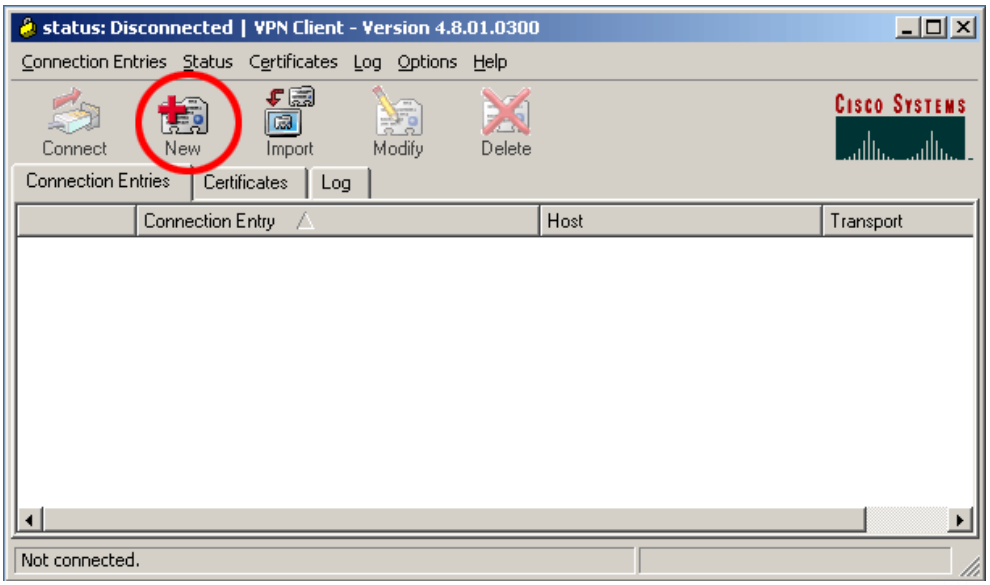
18、查看配置汇总信息：



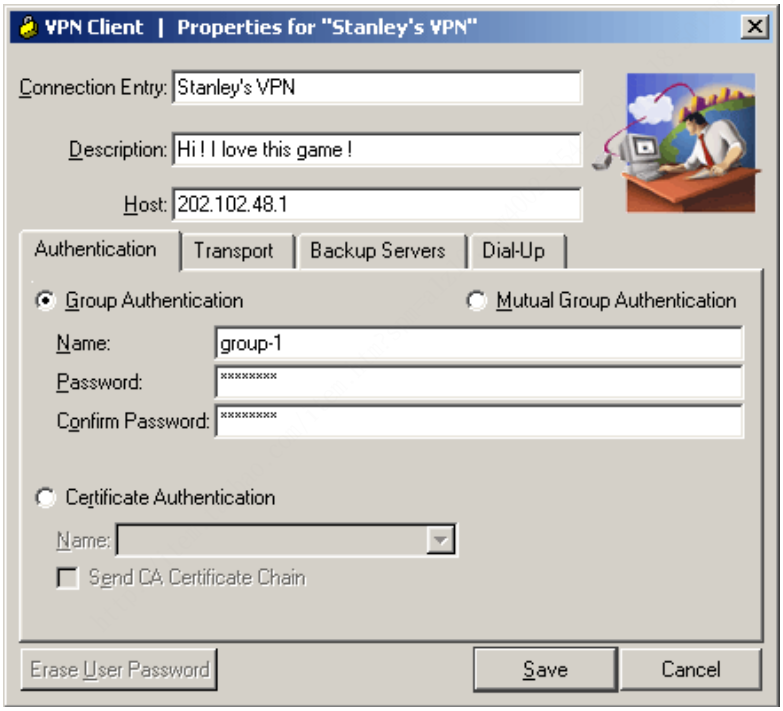
19、将生成的配置写入到路由器：



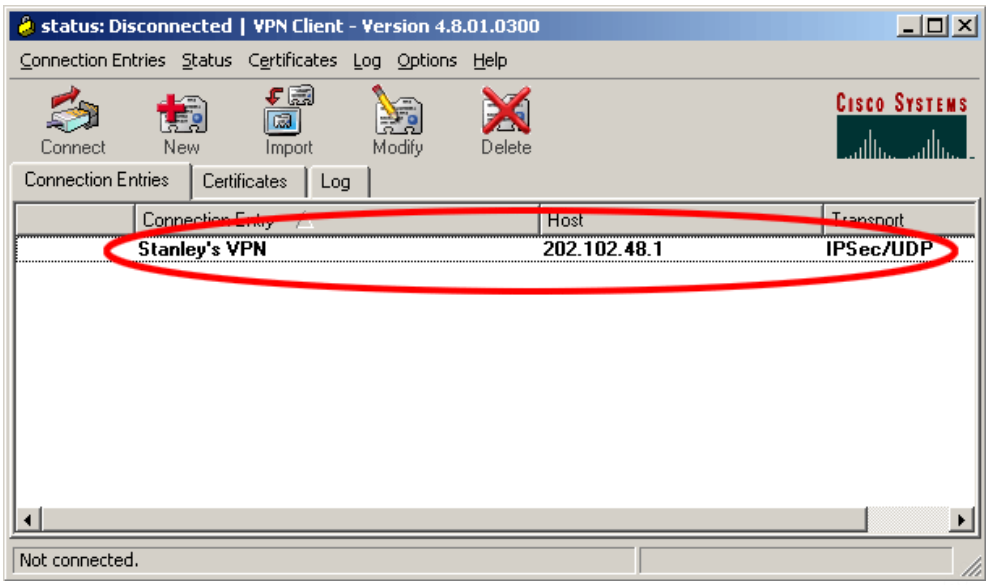
20、为了测试 Easy VPN 的配置正确性，需要在客户端安装 Cisco Easy VPN Client 软件，同时创建新连接，下面为客户端主界面：



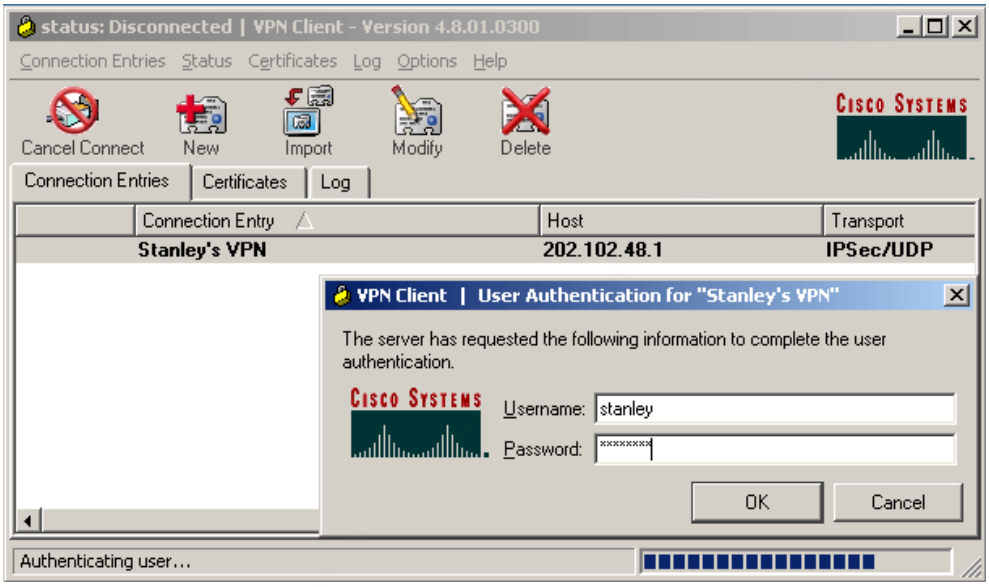
21、建立新的连接图示，并且填写 VPN SERVER 的主机地址和相应的客户组的组名和认证密码：



22、查看并双击进行连接：

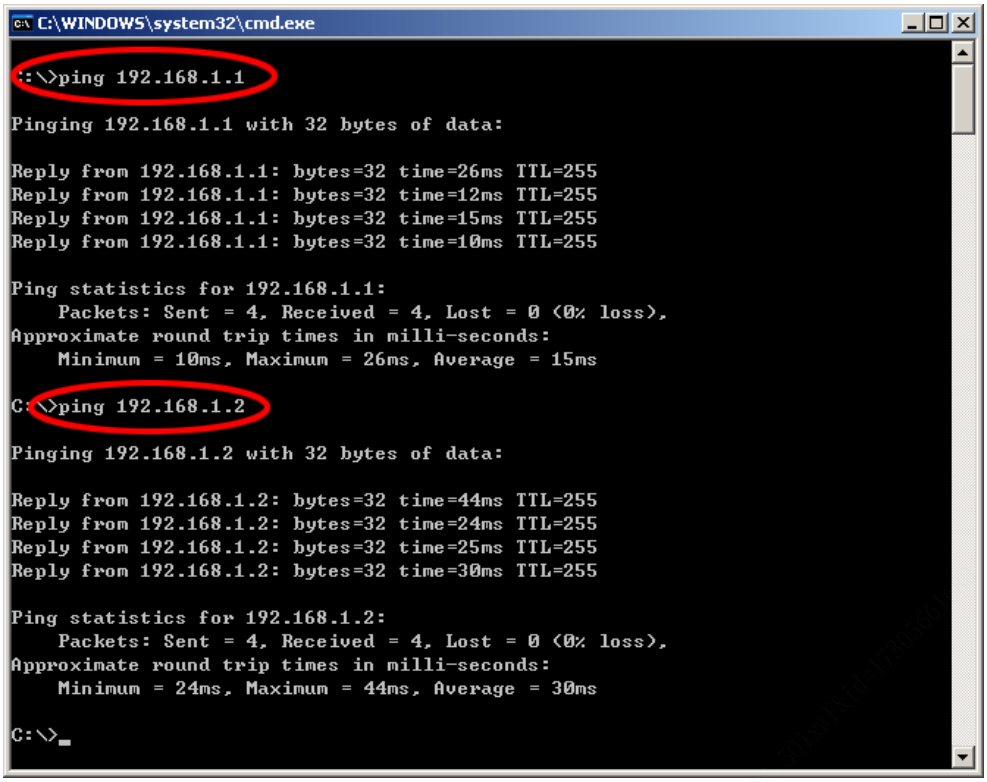


22、组认证成功后，需要提供 Easy VPN 的客户端的帐号和密码：



23、观察任务栏右下角的图示，确认连接成功：

24、在客户端开启命令行窗口，使用 ping 命令确认可以与内部网络服务器进行通讯：



25、使用 telnet 命令确认，可以连接到内部网络：

26、查看 R1 路由器生成的配置命令：

```
R2#show running-config
Building configuration...

..............
hostname R2
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization network sdm_vpn_group_ml_1 local
!
```

```
aaa session-id common
!
username wangyuan privilege 15 password 0 cisco
username stanley secret 5 $1$8h8K$pqZqXV.YSY72iSj9a1CmN1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group group-1
 key cisco
 dns 1.1.1.1
 wins 2.2.2.2
 pool SDM_POOL_1
 acl 100
 max-users 10
 max-logins 1
!
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto dynamic-map SDM_DYNMAP_1 1
 set transform-set ESP-3DES-SHA
 reverse-route
!
!
crypto map SDM_CMAP_1 client authentication list sdm_vpn_xauth_ml_1
crypto map SDM_CMAP_1 isakmp authorization list sdm_vpn_group_ml_1
crypto map SDM_CMAP_1 client configuration address respond
crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1
!
interface FastEthernet0/0
 ip address 202.102.48.1 255.255.255.0
 duplex half
 no cdp enable
 crypto map SDM_CMAP_1
!
ip local pool SDM_POOL_1 172.16.1.1 172.16.1.10
ip http server
!
access-list 100 remark SDM_ACL Category=4
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
```

批注 [stanley727]： SDM 产生的 VPN 帐号。

批注 [stanley728]： 组的密钥配置，客户端的 DNS 配置，Wins 服务器 IP 地址，隧道分离，地址池调用，最大用户在线数以及每个用户同时会话数量的定义。

批注 [stanley729]： 反向路由注入。

批注 [stanley730]： 配置客户端的 xauth 认证列表，选择组授权列表，响应客户端的地址请求。

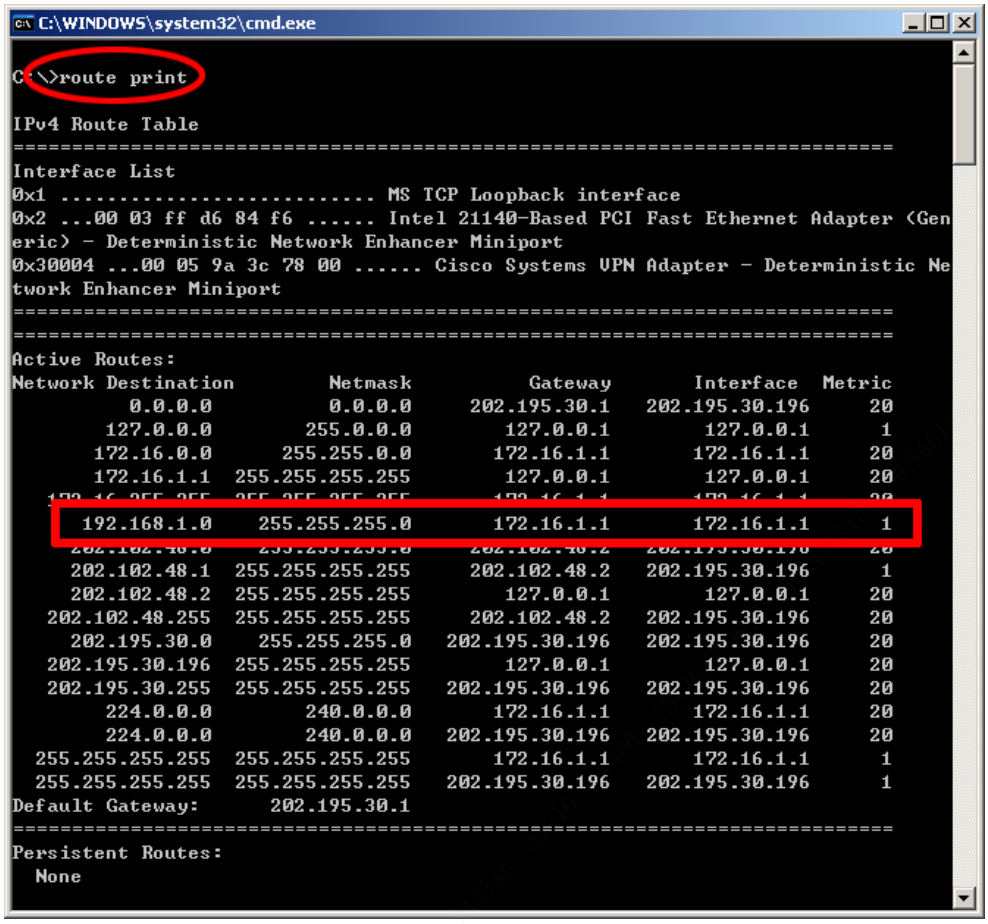
批注 [stanley731]： 客户端地址汇的配置。

批注 [stanley732]： 隧道分离的 ACL 配置。

```
end

R2#
```

27、查看客户端的路由表，确认隧道分离的反向路由注入：



```
C:\WINDOWS\system32\cmd.exe

C:\>route print

IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 03 ff d6 84 f6 ...... Intel 21140-Based PCI Fast Ethernet Adapter (Gen
eric) - Deterministic Network Enhancer Miniport
0x30004 ...00 05 9a 3c 78 00 ...... Cisco Systems VPN Adapter - Deterministic Ne
twork Enhancer Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     202.195.30.1   202.195.30.196     20
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
      172.16.0.0      255.255.0.0      172.16.1.1       172.16.1.1     20
      172.16.1.1  255.255.255.255        127.0.0.1        127.0.0.1     20
    192.168.1.0    255.255.255.0      172.16.1.1       172.16.1.1      1
    202.102.48.1  255.255.255.255     202.102.48.2   202.195.30.196      1
    202.102.48.2  255.255.255.255        127.0.0.1        127.0.0.1     20
  202.102.48.255  255.255.255.255     202.102.48.2   202.195.30.196     20
    202.195.30.0    255.255.255.0   202.195.30.196   202.195.30.196     20
  202.195.30.196  255.255.255.255        127.0.0.1        127.0.0.1     20
  202.195.30.255  255.255.255.255   202.195.30.196   202.195.30.196     20
        224.0.0.0        240.0.0.0      172.16.1.1       172.16.1.1     20
        224.0.0.0        240.0.0.0   202.195.30.196   202.195.30.196     20
  255.255.255.255  255.255.255.255      172.16.1.1       172.16.1.1      1
  255.255.255.255  255.255.255.255   202.195.30.196   202.195.30.196      1
Default Gateway:      202.195.30.1
===========================================================================
Persistent Routes:
  None
```

28、查看客户端的 IP 配置：

```
C:\>ipconfig /all

Windows IP Configuration
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Cisco Systems VPN Adapter
   Physical Address. . . . . . . . . : 00-05-9A-3C-78-00
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 172.16.1.1
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
```

批注 [stanley733]：从服务器端获得的动态 IP 地址。

```
   DNS Servers . . . . . . . . . . . : 1.1.1.1
   Primary WINS Server . . . . . . . : 2.2.2.2

C:\>
```

批注 [stanley734]: 从服务端获得的 DNS 和 WINs 的地址。

29、查看 R1 路由器路由表：

```
R2#show ip route

Gateway of last resort is not set

C    202.102.48.0/24 is directly connected, FastEthernet0/0
     172.16.0.0/32 is subnetted, 1 subnets
S       172.16.1.1 [1/0] via 202.102.48.2
C    192.168.1.0/24 is directly connected, Serial1/0
R2#
```

批注 [stanley735]: 到客户端的路由条目。

29、实验完成。

CCNP Lab Manual

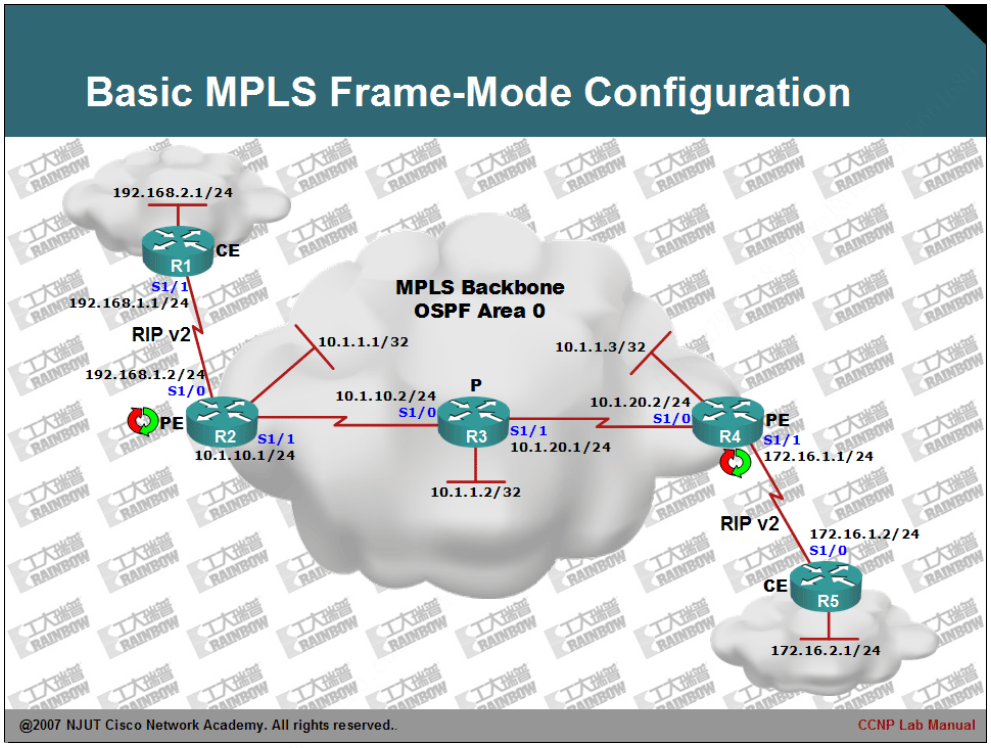
Lab 66. Basic MPLS Frame-Mode Configuration

实验目的：

1、掌握帧模式的 MPLS 基本配置。

2、理解 MPLS 的的标签过程。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。

2、配置 MPLS 骨干区域 OSPF 路由。并使用 show ip route 命令确认 OSPF 路由由已经收敛。需要注意的是 R2 的 loopback 0 的接口，其子网掩码是 32 位的。其目的是用作于 BGP 的会话的更新源和 LDP 路由器的 ID。

```
R2(config)#interface loopback 0
R2(config-if)#ip address 10.1.1.1 255.255.255.255
R2(config-if)#exit
R2(config)#router ospf 100
R2(config-router)#router-id 10.1.1.1
R2(config-router)#network 10.1.1.1 0.0.0.0 area 0
R2(config-router)#network 10.1.10.0 0.0.0.255 area 0
R2(config-router)#exit
```

批注 [stanley736]：手工指定 ospf 路由的 router-id

批注 [stanley737]：将其加入到 OSPF 的进程，以便于后面使用其创建 BGP 的会话。

在 LOOPBACK 0 口配置 32 位地址原因：这是因为 OSPF 在默认通告环回口时，会将其通告为 32 位掩码的 IP 地址。而其它 LSR（标签交换路由器）会创建一个与 PE 路由器通告的 OSPF 相对应的标签绑定(OSPF Router-ID 与 LDP Router-ID)，即使用 32 位掩码的路由。但是由于 PE 路由器的与标签绑定的接口 LOOPBACK 0 实际为 24 位，则会出现 LSP（标签转发协议）出错，导致 MPLS 不能正常的工作。也可以采用如下的配置，确保 ID 相同。

```
R2(config)#interface loopback 0
R2(config-if)#ip ospf default network point-to-point
R2(config-if)#exit
```

批注 [stanley738]：这是一种替代的办法。但是不推荐这样去做。

3、配置 MPLS 的 PE 路由器 R2，PE 全称为 Provide Edge。

4、首先在 R2 上启用 CEF。**CISCO 的 MPLS 依赖于 CEF，因此必须启用 CEF 的快速转发机制。**

```
R2(config)#ip cef
```

5、配置 R2 的标签转发协议。

```
R2(config)#mpls label protocol ldp
```

批注 [stanley739]：MPLS 有两种标签转发协议 TDP(CISCO 私有)和 LDP。CISCO 默认的标签分发协议为 TDP。

6、配置 TDP/LDP 的路由器 ID。配置 ID 的主要目的是为了方便排错。

```
R2(config)#interface s1/1
R2(config-if)#mpls ip
R2(config-if)#tag-switching ip
R2(config-if)#exit
```

批注 [stanley740]：接口启用 MPLS。

批注 [stanley741]：启用标签转发。

8、配置 PE 路由器 R4 的 MPLS:

```
R4(config)#ip cef
R4(config)#mpls label protocol ldp
R4(config)#mpls ldp router-id loopback 0 force
R4(config)#
R4(config)#interface serial 1/0
R4(config-if)#mpls ip
R4(config-if)#tag-switching ip
R4(config-if)#exit
R4(config)#exit
```

9、配置 P 路由器 R3。

```
R3(config)#ip cef
R3(config)#mpls label protocol ldp
R3(config)#mpls ldp router-id loopback 0 force
R3(config)#
R3(config)#interface serial 1/0
R3(config-if)#mpls ip
R3(config-if)#tag-switching ip
R3(config-if)#exit
R3(config)#
R3(config)#interface serial 1/1
R3(config-if)#mpls ip
R3(config-if)#tag-switching ip
R3(config-if)#exit
R3(config)#exit
R3#
```

10、在配置过程中，当在 R2 的 S1/1 和 S1/2 的接口分配启用了 MPLS 和标签协议后，会在 R2 上出现如下的系统提示信息：

```
*Jun  3 15:32:20.371: %LDP-5-NBRCHG: LDP Neighbor 10.1.1.1:0 is UP
*Jun  3 15:32:31.823: %LDP-5-NBRCHG: LDP Neighbor 10.1.1.3:0 is UP
```

11、在 R1 和 R2 的接口查看 MPLS 的接口工作信息。

```
R3#show mpls interfaces
Interface              IP           Tunnel   Operational
Serial1/0              Yes (ldp)    No       Yes
Serial1/1              Yes (ldp)    No       Yes
```

```
R2#show mpls interfaces
Interface              IP           Tunnel   Operational
Serial1/1              Yes (ldp)    No       Yes
R2#
```

批注 [stanley742]： 此信息表示，MPLS 的 LDP 协议已经发现其邻居 LSR。
此时，MPLS 的 LSR 会主动的向邻居通告标签。

标签通告的两种方式：
主动下游标签分发
下游按需标签分发

当上游向下流分发标签时，默认情况下，下流 LSR 会忽略。其依赖于标签保留的模式：
1. 激进的标签保留
2. **保守的标签保留**

批注 [stanley743]： 此处显示 R3 上有两个接口参与到 MPLS 中。并且两个接口都使用 LDP 的协议。

12、在 R3 上查看 LDP 的邻居信息：

```
R3#show mpls ldp neighbor

    Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.2:0
        TCP connection: 10.1.1.1.646 - 10.1.1.2.40796
        State: Oper; Msgs sent/rcvd: 157/158; Downstream
        Up time: 01:51:43
        LDP discovery sources:
          Serial1/0, Src IP addr: 10.1.10.1
        Addresses bound to peer LDP Ident:
          192.168.1.2     10.1.10.1       10.1.1.1
    Peer LDP Ident: 10.1.1.3:0; Local LDP Ident 10.1.1.2:0
        TCP connection: 10.1.1.3.18305 - 10.1.1.2.646
        State: Oper; Msgs sent/rcvd: 155/157; Downstream
        Up time: 01:51:32
        LDP discovery sources:
          Serial1/1, Src IP addr: 10.1.20.2
        Addresses bound to peer LDP Ident:
          10.1.20.2       172.16.1.1      10.1.1.3
R3#
```

批注 [stanley744]： 邻居和本地的 LDP Router-ID

批注 [stanley745]： 646 标识了 LDP 协议通过 UDP/TCP 的 646 号端口用于邻居的发现和建立。

另外 LDP 使用 224.0.0.2 组播地址创建邻居。

TDP 协议使用 UDP/TCP 的 711 的端用于邻居的发现和建立，并且使用的广播的方式。

13、查看 R3 的 LDP 标签信息库，即 MPLS 的 LDP 生成的 LIB。

```
R3#show mpls ldp bindings

.....
  tib entry: 172.16.1.0/24, rev 20
        local binding:  tag: 21
        remote binding: tsr: 10.1.1.3:0, tag: imp-null
        remote binding: tsr: 10.1.1.1:0, tag: 21
  tib entry: 172.16.2.0/24, rev 34
        local binding:  tag: 20
        remote binding: tsr: 10.1.1.3:0, tag: 20
        remote binding: tsr: 10.1.1.1:0, tag: 20
  tib entry: 192.168.1.0/24, rev 17
        local binding:  tag: 18
        remote binding: tsr: 10.1.1.1:0, tag: imp-null
        remote binding: tsr: 10.1.1.3:0, tag: 21
  tib entry: 192.168.2.0/24, rev 32
        local binding:  tag: 19
        remote binding: tsr: 10.1.1.1:0, tag: 19
        remote binding: tsr: 10.1.1.3:0, tag: 19
.....
R2#
```

批注 [stanley746]： 针对 192.168.1.0/24 子网的标签信息。

批注 [stanley747]： 本地分配给该子网的标签绑定为 18.

批注 [stanley748]： 从对等体 LSR 10.1.1.1 和 10.1.1.3 接收到关于此子网的标签。

10.1.1.1 的 imp-null 表示下一跳路由器未对该此网分配标签。说明对于目标来说，本地路由器为倒数第二跳路由器。需要在本地进行剥离标签。其遵守 PHP 机制，即第二跳弹出机制。

10.1.1.3 分配的标签为 21

14、查看 R4 的 LIB。

```
R4#show mpls ldp bindings

.............
  tib entry: 172.16.2.0/24, rev 34
        local binding:  tag: 20
        remote binding: tsr: 10.1.1.2:0, tag: 20
  tib entry: 192.168.1.0/24, rev 18
        local binding:  tag: 21
        remote binding: tsr: 10.1.1.2:0, tag: 18
  tib entry: 192.168.2.0/24, rev 32
        local binding:  tag: 19
        remote binding: tsr: 10.1.1.2:0, tag: 19
.............
R2#
```

批注 [stanley749]：针对 192.168.1.0/24 子网的标签信息。

批注 [stanley750]：本地分配给该子网的标签绑定为 21。

批注 [stanley751]：从 10.1.1.2 收到的标签为 18。

15、查看 R2、R3 和 R4 的 FLIB，即标签转发信息库。

```
R2#show mpls forwarding-table

Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     10.1.1.2/32      0          Se1/1       point2point
17     16          10.1.1.3/32      0          Se1/1       point2point
18     Pop tag     10.1.20.0/24     0          Se1/1       point2point
19     Untagged    192.168.2.0/24   0          Se1/0       point2point
20     20          172.16.2.0/24    0          Se1/1       point2point
21     21          172.16.1.0/24    0          Se1/1       point2point
R2#
```

```
R3#show mpls forwarding-table

Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     10.1.1.3/32      0          Se1/1       point2point
17     Pop tag     10.1.1.1/32      0          Se1/0       point2point
18     Pop tag     192.168.1.0/24   0          Se1/0       point2point
19     19          192.168.2.0/24   0          Se1/0       point2point
20     20          172.16.2.0/24    0          Se1/1       point2point
21     Pop tag     172.16.1.0/24    0          Se1/1       point2point
R3#
```

批注 [stanley752]：POP 表示，弹出标签。即 PHP 的机制，其目的是避免在 MPLS 的 PE 路由器上执行 FLIB 的检索。而是强制 PE 路由器直接对路由表检索后转发该数据包。

```
R4#show mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	10.1.10.0/24	0	Se1/0	point2point
17	Pop tag	10.1.1.2/32	0	Se1/0	point2point
18	17	10.1.1.1/32	0	Se1/0	point2point
19	19	192.168.2.0/24	0	Se1/0	point2point
20	Untagged	172.16.2.0/24	0	Se1/1	point2point
21	**18**	**192.168.1.0/24**	**0**	**Se1/0**	**point2point**

R4#

14、使用标签进行路由的简单过程：

1）R4 收到一个需要到达 192.168.1.0/24 网络的数据包

2）R4 检查本地的 FLIB 后,为数据包打上 18 的标签，编号为 18 标签为上游邻居通告的，即 R3 路由器。

3）根据 FLIB，R4 从 s1/0 的接口转发被打上标签的数据包。

4）R3 路由器收到一个被打上标签为 18 的数据包。

5）R3 检查本地 FLIB 后，发现针对 18 的标签，应该进行 POP 的标签剥离。

6）R3 剥离标签后，将 IP 数据包按 FLIB 所示从本地 s1/0 接口转发出去。

7）R2 收到一个没有打标签的数据包，R2 查询 IP 路由表，确定下一跳为 192.168.1.1。

8）R2 根据 IP 路由表，将数据包转发给下一跳路由器 192.168.1.1。

9）结束。

15、查看一些关于 MPLS 的 LDP 的参数信息。

```
R2#show mpls ldp parameters

Protocol version: 1
Downstream label generic region: min label: 16; max label: 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
Downstream on Demand Path Vector Limit: 255
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
```

批注 [stanley753]: 1-15 的标签为保留的标签号。

```
R2#
```

16、在 R1 上使用 PING 命令，确认网络。

```
R1#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 240/293/336 ms
R1#
```

17、实验完成。

CCNP Lab Manual

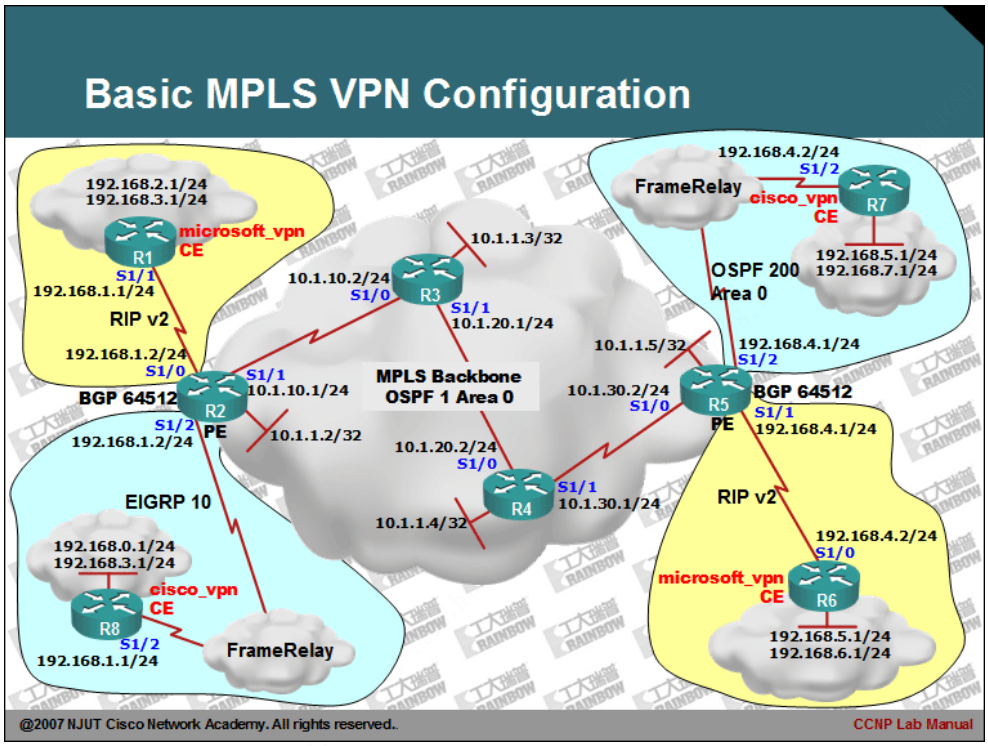
Lab 67. Basic MPLS VPN Configuration

实验目的：

1、掌握基本的 MPLS-VPN 配置方法.

2、理解 MPLS-VPN 如何解决地址空间重叠问题。

实验拓扑图：



实验步骤及要求：

1、由于本实验中存在两个不同的 VPN 的场点，Microsoft VPN 和 Cisco VPN，而且两个场点都使用 192.168.0.0/16 的相同的无类子网空间，同时部分地址同时存在于两个 VPN 的场点中。另外本实验配置命令过多，为了避免实验失败，所以在配置本实验时，请 NP 学员按照步骤完成实验。如果您对 MPLS 的非常熟悉，则可以按照自己意愿任意配置。

2、首先配置 R1、R2、R3、R4、R5、R6 的接口 IP，并且确保直连接口相互可以 PING 通。

3、配置 MPLS 骨干的 IGP 路由器，本实验采用 OSPF 路由协议，也可以采用 ISIS。不过需要注意的是目前仅有 OSPF 和 ISIS 支持 MPLS 的流量工程。下面给个 R2 的配置范例，关于 R3 和 R4 以及 R5 的配置，请各位自行补齐。

```
R2(config)#router ospf 100
R2(config-router)#passive-interface loopback 0
R2(config-router)#router-id 10.1.1.2
R2(config-router)#network 10.0.0.0 0.255.255.255 area 0
R2(config-router)#exit
R2(config)#
```

批注 [stanley754]：汇总的 OSPF 的宣告接口的方式。本条命令，可以一次将 R2 的 S1/1 接口和 Loopback0 接口，一次性加入到 OSPF 的进程。

4、查看 MPLS 骨干路由器的路由表，以确认每一台的路由器其 OSPF 工作正常。

```
R2#show ip route

.........
O       10.1.1.3/32 [110/65] via 10.1.10.2, 00:00:44, Serial1/1
O       10.1.1.4/32 [110/129] via 10.1.10.2, 00:00:44, Serial1/1
O       10.1.1.5/32 [110/193] via 10.1.10.2, 00:00:44, Serial1/1
O       10.1.30.0/24 [110/192] via 10.1.10.2, 00:00:44, Serial1/1
O       10.1.20.0/24 [110/128] via 10.1.10.2, 00:00:44, Serial1/1
.........
R2#
```

5、配置 PE 路由器 R2 和 R5 的 MPLS。

```
R2(config)#ip cef
R2(config)#
R2(config)#mpls label protocol ldp
R2(config)#
R2(config)#mpls ldp router-id loopback 0 force
R2(config)#
R2(config)#interface serial 1/1
R2(config-if)#mpls ip
```

批注 [stanley755]：启用 CEF。

批注 [stanley756]：选择 LDP 标签分发协议。

批注 [stanley757]：选择使用回环口作为 LSR 的 Router-ID。

```
R2(config-if)#tag-switching ip
R2(config-if)#exit
R2(config)#
```

批注 [stanley758]：为 s1/1 接口启用 MPLS 的标签转发。

```
R5(config)#ip cef
R5(config)#mpls label protocol ldp
R5(config)#mpls ldp router-id loopback 0 force
R5(config)#interface serial 1/0
R5(config-if)#mpls ip
R5(config-if)#tag-switching ip
R5(config-if)#exit
R5(config)#
```

6、配置骨干路由器 P(Provider)，即 R3 和 R4 路由器的 MPLS。

```
R3(config)#ip cef
R3(config)#mpls label protocol ldp
R3(config)#mpls ldp router-id loopback 0 force
R3(config)#interface serial 1/1
R3(config-if)#mpls ip
R3(config-if)#tag-switching ip
R3(config-if)#exit
R3(config)#
R3(config)#interface serial 1/0
R3(config-if)#mpls ip
R3(config-if)#tag-switching ip
R3(config-if)#exit
R3(config)#exit
R3#
```

```
R4(config)#ip cef
R4(config)#mpls label protocol ldp
R4(config)#mpls ldp router-id loopback 0 force
R4(config)#interface serial 1/1
R4(config-if)#mpls ip
R4(config-if)#tag-switching ip
R4(config-if)#exit
R4(config)#
R4(config)#interface serial 1/0
R4(config-if)#mpls ip
R4(config-if)#tag-switching ip
R4(config-if)#exit
R4(config)#exit
R4#
```

7、在任意一台 MPLS 骨干路由器上查看 FLIB(标签转发表)，确认 MPLS 工作正常。

```
R2#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Untagged    10.1.1.3/32      0          Se1/1       point2point
17     Pop tag     10.1.20.0/24     0          Se1/1       point2point
18     17          10.1.1.4/32      0          Se1/1       point2point
19     19          10.1.30.0/24     0          Se1/1       point2point
20     18          10.1.1.5/32      0          Se1/1       point2point
R2#
```

8、在两台 PE 路由器上配置 BGP 协议。配置 BGP 协议的目的是为了启用 MP-BGP，用于在 PE 路由器之间交换 VPN 路由。由于 BGP 创建邻居时，不要求对等体是物理直连接的，因此 BGP 使用 TCP 179 号端口进行邻居的会话，因此本实验中，只需要配置 R2 与 R5 路由器的 BGP 协议。

```
R2(config)#router bgp 64512
R2(config-router)#neighbor 10.1.1.5 remote-as 64512
R2(config-router)#neighbor 10.1.1.5 update-source loopback 0
R2(config-router)#no synchronization
R2(config-router)#no auto-summary
R2(config-router)#exit
R2(config)#
```

```
R5(config)#router bgp 64512
R5(config-router)#neighbor 10.1.1.2 remote-as 64512
R5(config-router)#neighbor 10.1.1.2 update-source loopback 0
R5(config-router)#no synchronization
R5(config-router)#no auto-summary
R5(config-router)#exit
R5(config)#exit
R5(config)#
```

批注 [stanley759]: CISCO 强烈建议使用一个掩码为 32 的接口指定为 BGP 的更新源。因此如果不这样做的，MPLS VPN 或 MVPN 可通不能正常运行。

MVPN 为 Multicast VPN 的简称。

批注 [stanley760]: 关闭同步的规则，是因此本有一个 IGP 的协议在运行。

批注 [stanley761]: 关闭自动汇总，其目的是确保在后面的重发布时，重分发到 BGP 的路由不会是在主网络边界被汇总。

9、确认 BGP 的邻居创建成功。

```
R2#show ip bgp summary
BGP router identifier 10.1.1.2, local AS number 64512
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.1.5        4 64512       5       5        1    0    0 00:01:25        0
R2#
```

10、激活两台 PE 路由器 MP-BGP 协议，其目的是用于交换不同 VPN 场点的路由。

```
R2(config)#router bgp 64512
R2(config-router)#
R2(config-router)#address-family vpnv4
R2(config-router-af)#neighbor 10.1.1.5 activate
R2(config-router-af)#neighbor 10.1.1.5 send-community extended
R2(config-router-af)#no auto-summary
R2(config-router-af)#exit
R2(config-router)#exit
R2(config)#
```

批注 [stanley762]：要启用 MP-BGP 协议，必须在 VPNv4 的地址家族下激活。

批注 [stanley763]：用于激活 MP-BGP 的邻居的路由交换。

批注 [stanley764]：启用 BGP 扩展共用体交换。

```
R5(config)#router bgp 64512
R5(config-router)#
R5(config-router)#address-family vpnv4
R5(config-router-af)#neighbor 10.1.1.2 activate
R5(config-router-af)#neighbor 10.1.1.2 send-community extended
R5(config-router-af)#no auto-summary
R5(config-router-af)#exit
R5(config-router)#exit
R5(config)#
```

启用扩展共用体交换的目的是，为了 MP-BGP 携带路由区分符(RD)和起源场点属性。路由区分符，可以确保不同的 VPN 场点的路由是相对独立的。其可以确保 MP-BGP 为不同的 VPN 场点构建不同的 VRF(VPN Routing Forwarding)转发表。路由区分符(RD)可以解决客户端场点地址空间重叠的问题。另外路由目标(RT)也可以实现与 RD 相同的功能。但 RD 灵活性不够，无法在 MPLS VPN 主干上支持复杂的网络拓扑。典型的一个案例，是不同的 VPN 场点相互的 VOIP 的实现时。可以使用 RT 解决不同的场点共用相同的一个语音网关。而此功能是 RD 无法实现的。

11、查看 R2 或是 R5 的 MP-BGP 协议状态，此外会发现在目前 MP-BGP 并没有为 VPN 场点产生任何相关的路由。

```
R2#show ip bgp vpnv4 all

R2#
```

12、配置 VRF，即 VPN 路由转发表，其实质是配置路由目标(RT)和路由区分符(RD)。而且需要注意的属于同一个 VPN 场点中的路由目标(RT)，其值必须一致。否则可能会导致 MPLS VPN 的路由表构建出错。

```
R2(config)#ip vrf microsoft_vpn
```

批注 [stanley765]：配置 microsoft_vpn 场点的路由目标标记。

注意:VRF 的名称是区分大小写的。

```
R2(config-vrf)#rd 64512:100
R2(config-vrf)#route-target import 64512:100
R2(config-vrf)#route-target export 64512:100
R2(config-vrf)#exit
R2(config)#exit
```

批注 [stanley766]：配置 microsoft_vpn 场点的路由区分符值为 64512：100。其使用的是 ASN：XX 格式。RD 有三种不同的模式。具体请参照相关书籍。

批注 [stanley767]：该命令指定将路由目标为 64512:100 的路由导入到 VRF 中。

批注 [stanley768]：指出从客户端的路由器重发布到 MP-BGP 中使用路由区分符为 64512:100。

```
R5(config)#ip vrf microsoft_vpn
R5(config-vrf)#rd 64512:100
R5(config-vrf)#route-target import 64512:100
R5(config-vrf)#route-target export 64512:100
R5(config-vrf)#exit
R5(config)#
```

13、分配在 R2 与 R5 路由器上配置 VRF 与接口关联性。

```
R2(config)#interface serial 1/0
R2(config-if)#ip vrf forwarding microsoft_vpn
% Interface Serial1/0 IP address 192.168.1.2 removed due to enabling VRF microsoft_vpn
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#exit
R2(config)#
```

批注 [stanley769]：将 microsoft_vpn 的 VRF 与 S1/0 接口关联起来。

批注 [stanley770]：由于配置了 VRF 会导致接口的 IP 丢失。因此需要重新配置一次 IP 地址。

```
R5(config)#interface serial 1/1
R5(config-if)#ip vrf forwarding microsoft_vpn
% Interface Serial1/1 IP address 192.168.4.1 removed due to enabling VRF microsoft_vpn
R5(config-if)#ip address 192.168.4.1 255.255.255.0
R5(config-if)#exit
R5(config)#exit
R5(config)#
```

14、确认 VRF 的详细信息。也可以使用 show ip vrf 命令，查看简单的 VRF 信息。

```
R5#show ip vrf detail
VRF microsoft_vpn; default RD 64512:100; default VPNID <not set>
  Interfaces:
    Se1/1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:64512:100
  Import VPN route-target communities
    RT:64512:100
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
R5#
```

批注 [stanley771]：VRF 的名称，以及 VRF 中配置的 RT 的值。

批注 [stanley772]：VRF 的工作接口。

```
R5#
```

15、配置 PE 与 CE 之间的路由选择协议和 MP-BGP 与 RIP 之间的路由重分发。目前需要配置的是 R2 与 R1，R5 与 R6 之间的路由选择协议，当然也可以配置静态路由。本实验采用 RIPv2 协议进行配置。

首先配置 CE 端的 RIP 路由。

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#network 192.168.3.0
R1(config-router)#exit
R1(config)#exit
R1#
```

```
R6(config)#router rip
R6(config-router)#version 2
R6(config-router)#network 192.168.4.0
R6(config-router)#network 192.168.5.0
R6(config-router)#network 192.168.6.0
R6(config-router)#exit
R6(config)#
```

其次再配置 PE 端的 RIP 路由。

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#
R2(config-router)#address-family ipv4 vrf microsoft_vpn
R2(config-router-af)#version 2
R2(config-router-af)#redistribute bgp 64512 metric transparent
R2(config-router-af)#network 192.168.1.0
R2(config-router-af)#no auto-summary
R2(config-router-af)#exit
R2(config-router)#exit
```

```
R5(config)#router rip
R5(config-router)#version 2
R5(config-router)#
R5(config-router)#address-family ipv4 vrf microsoft_vpn
R5(config-router-af)#version 2
R5(config-router-af)#network 192.168.4.0
R5(config-router-af)#redistribute bgp 64512 metric transparent
R5(config-router-af)#no auto-summary
```

批注 [stanley773]： 配置为 V2 的 RIP 版本。

批注 [stanley774]： 启用 IPV4 地址家族，配置 RIP 与 VRF 表转发表之间的关系。其指出在重分布时的采用 VRF 中那个 RT 的值。

批注 [stanley775]： 将 MP-BGP 中的带有 64512：100 的 RT 的路由重发布到 RIP 中。

Transparent 的关键字，主要的目的是保留 RIP 的原始的度量值。他们是被复制在 MED 属性中的。

```
R5(config-router-af)#exit
R5(config-router)#exit
R5(config)#
```

然后再配置 BGP，确保 RIP 的路由重发布到 MP-BGP 中。

```
R2(config)#router bgp 64512
R2(config-router)#
R2(config-router)#address-family ipv4 vrf microsoft_vpn
R2(config-router-af)#redistribute rip
R2(config-router-af)#no auto-summary
R2(config-router-af)#no synchronization
R2(config-router-af)#exit
R2(config-router)#exit
R2(config)#exit
```

批注 [stanley776]：配置重发布时的 VRF 相关联的 RT 的值。

批注 [stanley777]：重发布 RIP 路由协议。

```
R5(config)#router bgp 64512
R5(config-router)#
R5(config-router)#address-family ipv4 vrf microsoft_vpn
R5(config-router-af)#redistribute rip
R5(config-router-af)#no synchronization
R5(config-router-af)#no auto-summary
R5(config-router-af)#exit
R5(config-router)#exit
R5(config)#
```

16、查看 microsoft_vpn 场点中的 R1 和 R6 路由器的路由表，确认 MPLS VPN 配置成功。

```
R1#show ip route

Gateway of last resort is not set

.....
R    192.168.4.0/24 [120/1] via 192.168.1.2, 00:00:23, Serial1/1
R    192.168.5.0/24 [120/2] via 192.168.1.2, 00:00:23, Serial1/1
R    192.168.6.0/24 [120/2] via 192.168.1.2, 00:00:23, Serial1/1
.....
R1#
```

批注 [stanley778]：R1 已经学习到 R6 路由器的路由。

```
R6#show ip route

Gateway of last resort is not set

.....
```

```
R     192.168.1.0/24 [120/1] via 192.168.4.1, 00:00:17, Serial1/0
R     192.168.2.0/24 [120/2] via 192.168.4.1, 00:00:17, Serial1/0
R     192.168.3.0/24 [120/2] via 192.168.4.1, 00:00:17, Serial1/0
.....

R6#
```

17、使用 PING 命令确认路由的有效性。

```
R1#ping 192.168.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 336/424/480 ms
R1#
```

批注 [stanley779]：通过 PING 可以看出路由是有效的。

```
R6#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 288/438/552 ms
R6#
```

18、关于 MPLS 的标签交换协议的相关调试输出信息，请具体参照实验手册：Basic MPLS Frame-Mode Configurationg 的实验一节。

19、查看 MP-BGP 关于 microsoft_vpn 场点的路由信息表。

```
R2#show ip bgp vpnv4 vrf microsoft_vpn
BGP table version is 13, local router ID is 10.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 64512:100 (default for vrf microsoft_vpn)
*> 192.168.1.0      0.0.0.0                  0         32768 ?
*> 192.168.2.0      192.168.1.1              1         32768 ?
*> 192.168.3.0      192.168.1.1              1         32768 ?
*>i192.168.4.0      10.1.1.5                 0    100      0 ?
*>i192.168.5.0      10.1.1.5                 1    100      0 ?
*>i192.168.6.0      10.1.1.5                 1    100      0 ?
R2#
```

批注 [stanley780]：MP-BGP 学习到的远端的 microsoft_vpn 场点的路由。

20、到此 microsoft_vpn 场点的 VPN 配置完成。下面需要实现的是 cisco_vpn 场点的 VPN 的配置。

21、配置 R8 路由器 IP 地址，并且启用 EIGRP 路由协议。其中关于 Frame-Relay 的配置如下：

```
R8(config)#interface serial 1/2
R8(config-if)#encapsulation frame-relay
R8(config-if)#no frame-relay inverse-arp
R8(config-if)#frame-relay map ip 192.168.1.2 802 broadcast
R8(config-if)#no shutdown
R8(config-if)#exit
R8(config)#
R8(config)#router eigrp 10
R8(config-router)#no auto-summary
R8(config-router)#network 192.168.0.0
R8(config-router)#network 192.168.1.0
R8(config-router)#network 192.168.3.0
R8(config-router)#exit
R8(config)#exit
```

批注 [stanley781]：客户端启用 EIGRP 的自治系统 10。

22、配置 PE 路由器 R2 的 S1/2 接口，并且一定要使用 PING 命令检测接口。配置如下：

```
R2(config)#interface serial 1/2
R2(config-if)#encapsulation frame-relay
R2(config-if)#no frame-relay inverse-arp
R2(config-if)#frame-relay map ip 192.168.1.1 208 broadcast
R2(config-if)#ip add 192.168.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

23、在 PE 路由器 R2 上，为 cisco_vpn 场点配置 VRF 表。

```
R2(config)#ip vrf cisco_vpn
R2(config-vrf)#rd 64512:200
R2(config-vrf)#route-target import 64512:200
R2(config-vrf)#route-target export 64512:200
R2(config-vrf)#exit
```

批注 [stanley782]：为 cisco_vpn 场点配置其路由目标(RT)值为 200。

24、配置 R2 的 EIGRP 协议。

```
R2(config)#router eigrp 100
R2(config-router)#no auto-summary
R2(config-router)#address-family ipv4 vrf cisco_vpn
R2(config-router-af)#redistribute bgp 64512 metric 10000 10 255 1 1500
```

批注 [stanley783]：启用 EIGRP 的 100 的自治系统。注意：此处的自治系统编号与 CE 端并不一定需要一致。

批注 [stanley784]：启用于 cisco_vpn 相关的 ipv4 地址家族。

```
R2(config-router-af)#network 192.168.1.0
R2(config-router-af)#no auto-summary
R2(config-router-af)#autonomous-system 10
R2(config-router-af)#exit
R2(config-router)#exit
```

批注 [stanley785]: 指定客户 VPN 的 EIGRP 的自治系统号。如果与 CE 的路由器不一致将不会创建邻居。

25、将 cisco_vpn 的 VRF 配置到相应场点接口上。

```
R2(config)#interface serial 1/2
R2(config-if)#ip vrf forwarding cisco_vpn
% Interface Serial1/2 IP address 192.168.1.2 removed due to enabling VRF cisco_vpn
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#exit
R2(config)#exit
```

26、查看 EIGRP 的 PE 与 CE 之间的邻居关系。

```
R2#show ip eigrp vrf cisco_vpn 10 neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.1.1             Se1/2            122 00:01:54   64   384  0  2
R2#
```

27、根据 VRF 配置 EIGRP 的路由重发布到 MP-BGP 中。

```
R2(config)#router bgp 64512
R2(config-router)#address-family ipv4 vrf cisco_vpn
R2(config-router-af)#redistribute eigrp 10
R2(config-router-af)#no auto-summary
R2(config-router-af)#no synchronization
R2(config-router-af)#exit
R2(config-router)#exit
R2(config)#
```

28、查看 MP-BGP 关于 cisco_vpn 场点的路由信息表

```
R2#show ip bgp vpnv4 vrf cisco_vpn
BGP table version is 19, local router ID is 10.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 64512:200 (default for vrf cisco_vpn)
*> 192.168.0.0      192.168.1.1         2297856         32768 ?
*> 192.168.1.0      0.0.0.0                   0         32768 ?
*> 192.168.3.0      192.168.1.1         2297856         32768 ?
R2#
```

29、配置 R7 路由器的 IP 地址和启用 OSPF 的路由协议。

```
R7(config)#interface serial 1/2
R7(config-if)#ip address 192.168.4.2 255.255.255.0
R7(config-if)#encapsulation frame-relay
R7(config-if)#frame-relay map ip 192.168.4.1 705 broadcast
R7(config-if)#no frame-relay inverse-arp
R7(config-if)#ip ospf network broadcast
R7(config-if)#exit
R7(config)#router ospf 100
R7(config-router)#redistribute bgp 64512 subnets
R7(config-router)#network 192.168.5.0 0.0.0.255 area 0
R7(config-router)#network 192.168.7.0 0.0.0.255 area 0
R7(config-router)#network 192.168.4.0 0.0.0.255 area 0
R7(config-router)#exit
```

30、在 PE 路由器 R5 上，为 cisco_vpn 场点配置 VRF 表。

```
R5(config)#ip vrf cisco_vpn
R5(config-vrf)#rd 64512:200
R5(config-vrf)#route-target import 64512:200
R5(config-vrf)#route-target export 64512:200
R5(config-vrf)#exit
```

31、配置 R5 的 S1/2 接口的 IP 地址和 OSPF 路由协议。

```
R5(config)#
R5(config)#
R5(config)#interface s1/2
R5(config-if)#ip ospf network broadcast
R5(config-if)#encapsulation frame-relay
R5(config-if)#no frame-relay inverse-arp
R5(config-if)#frame-relay map ip 192.168.4.2 507 broadcast
R5(config-if)#ip vrf forwarding cisco_vpn
R5(config-if)#ip add 192.168.4.1 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#exit
R5(config)#
R5(config)#router ospf 200 vrf cisco_vpn
R5(config-router)#network 192.168.4.0 0.0.0.255 area 0
R5(config-router)#redistribute bgp 64512 subnets
R5(config-router)#exit
R5(config)#
```

批注 [stanley786]: OSPF 直接使用进程号与 VRF 进行关联。而不使用 IPv4 的地址家族的配置方法。

32、配置在 MP-BGP 中重发布 CE 端的 OSPF 路由。

```
R5(config)#router bgp 64512
R5(config-router)#address-family ipv4 vrf cisco_vpn
```

```
R5(config-router-af)#redistribute ospf 200
R5(config-router-af)#no auto-summary
R5(config-router-af)#no synchronization
R5(config-router-af)#exit
R5(config-router)#exit
R5(config)#
```

33、查看 cisco_vpn 场点中的 R8 或是 R7 路由器的路由表。

```
R7#show ip route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial1/2
C    192.168.5.0/24 is directly connected, Loopback0
C    192.168.7.0/24 is directly connected, Loopback1
O E2 192.168.0.0/24 [110/2297856] via 192.168.4.1, 00:06:10, Serial1/2
O E2 192.168.1.0/24 [110/1] via 192.168.4.1, 00:06:10, Serial1/2
O E2 192.168.3.0/24 [110/2297856] via 192.168.4.1, 00:06:10, Serial1/2
R7#
```

批注 [stanley787]: 通过 VPN 通道学习到路由。

34、使用 PING 命令检测路由有效性。

```
R7#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 424/483/576 ms
R7#
```

35、在任意 PE 路由器上查看 MP-BGP 的信息库。

```
R2#show ip bgp vpnv4 all
BGP table version is 34, local router ID is 10.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 64512:100 (default for vrf microsoft_vpn)
*> 192.168.1.0      0.0.0.0                  0         32768 ?
*> 192.168.2.0      192.168.1.1              1         32768 ?
*> 192.168.3.0      192.168.1.1              1         32768 ?
*>i192.168.4.0      10.1.1.5                 0    100      0 ?
*>i192.168.5.0      10.1.1.5                 1    100      0 ?
*>i192.168.6.0      10.1.1.5                 1    100      0 ?
Route Distinguisher: 64512:200 (default for vrf cisco_vpn)
```

批注 [stanley788]: MP-BGP 为 microsoft_vpn 场点构建的路由表。

批注 [stanley789]: MP-BGP 为 cisco_vpn 场点构建的路由表。

```
*> 192.168.0.0      192.168.1.1      2297856         32768 ?
*> 192.168.1.0      0.0.0.0                0         32768 ?
*> 192.168.3.0      192.168.1.1      2297856         32768 ?
*>i192.168.4.0      10.1.1.5               0    100      0 ?
*>i192.168.5.1/32   10.1.1.5              65    100      0 ?
*>i192.168.7.1/32   10.1.1.5              65    100      0 ?
R2#
```

36、查看 microsoft_vpn 场点 R6 路由器与 cisco_vpn 场点 R7 路由器的路由表。

观察路由表，确认 MPLS VPN 可以切实有效的解决地址重叠的问题。

```
R6#show ip route

.............
C    192.168.4.0/24 is directly connected, Serial1/0
C    192.168.5.0/24 is directly connected, Loopback0
C    192.168.6.0/24 is directly connected, Loopback1
R    192.168.1.0/24 [120/1] via 192.168.4.1, 00:00:19, Serial1/0
R    192.168.2.0/24 [120/2] via 192.168.4.1, 00:00:19, Serial1/0
R    192.168.3.0/24 [120/2] via 192.168.4.1, 00:00:19, Serial1/0
R6#
```

```
R7#show ip route

.............
C    192.168.4.0/24 is directly connected, Serial1/2
C    192.168.5.0/24 is directly connected, Loopback0
C    192.168.7.0/24 is directly connected, Loopback1
O E2 192.168.0.0/24 [110/2297856] via 192.168.4.1, 00:12:16, Serial1/2
O E2 192.168.1.0/24 [110/1] via 192.168.4.1, 00:12:16, Serial1/2
O E2 192.168.3.0/24 [110/2297856] via 192.168.4.1, 00:12:16, Serial1/2
R7#
```

加粗显示的路由条目，用于区分不同的 VPN 的场点。

37、再次使用 PING 确认各个场点的路由表的路由有效性。此处不再列出结果。

38、实验完成。

CCNP Lab Manual

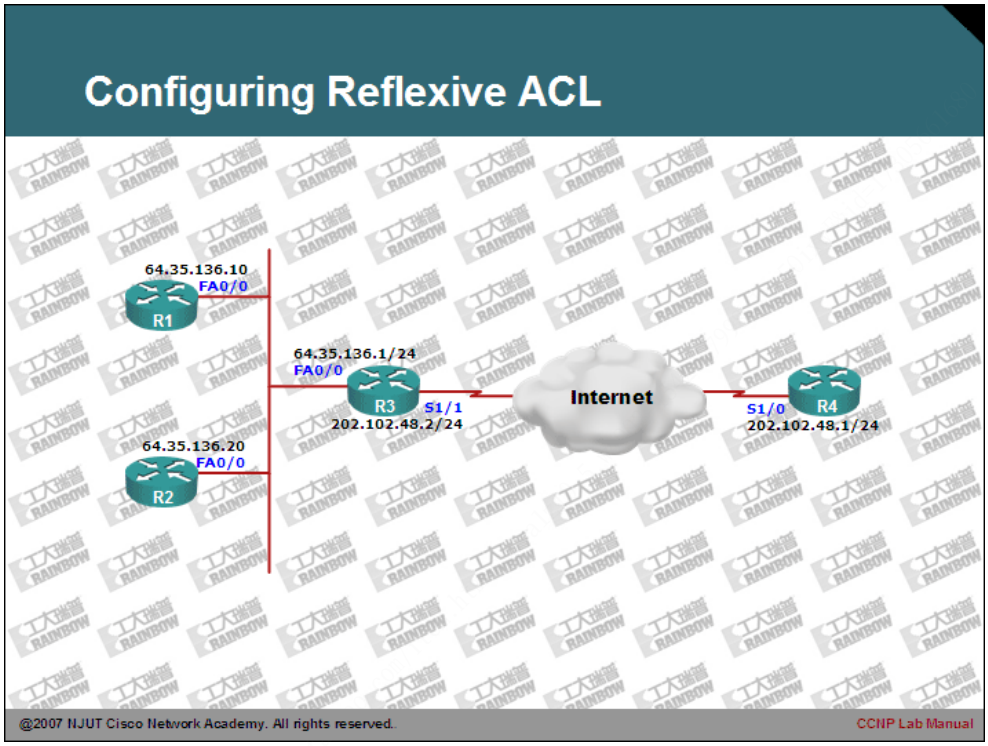
Lab 68. Configuring Reflexive ACL

实验目的：

1、掌握反射 ACL 的配置方法。

2、理解反射 ACL 的工作原理。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 Ping 命令确认各路由器的直连口的互通。同时在 R1、R2、R4 路由器上配置 VTY 线路，以便于进一步测试。

2、在 R1、R2 和 R4 上配置静态路由，确保网络可以相互访问。配置如下：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 64.35.136.1
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 64.35.136.1
```

```
R4(config)#ip route 64.35.136.0 255.255.255.0 202.102.48.2
```

4、在 R1、R2 和 R3 上使用 telnet 测试网络连接：

```
R4#telnet 64.35.136.10
Trying 64.35.136.10 ... Open
User Access Verification
Password: ******
R1>logout
[Connection to 64.35.136.10 closed by foreign host]
R4#
R4#
R4#telnet 64.35.136.20
Trying 64.35.136.20 ... Open
User Access Verification
Password: *******
R2>logout
[Connection to 64.35.136.20 closed by foreign host]
R4#
```

批注 [stanley790]: R4 可以使用 TELNET 访问 R1 路由器。

批注 [stanley791]: R4 可以使用 TELNET 访问 R2 路由器。

```
R1#telnet 202.102.48.1
Trying 202.102.48.1 ... Open
User Access Verification
Password: ******
R4>logout
 [Connection to 202.102.48.1 closed by foreign host]
R1#
R1#ping 202.102.48.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/176/240 ms
R1#
```

批注 [stanley792]: 内网的 R1 也可以使用 TELNET 访问 R4 路由器。

批注 [stanley793]: 同时 R1 也可以使用 PING 访问 R4 路由器。

R2 路由也与 R1 路由器可以访问 R4 路由器。

3、为了确保网络的安全，需要在 R3 上配置 ACL，拒绝由 Internet 路由器 R4 向

64.35.136.0/24 的网络发起任何访问。

4、为了完成要求，在 R3 上实施如下配置：

```
R3(config)#access-list 1 deny any
R3(config)#
R3(config)#interface s1/1
R3(config-if)#ip access-group 1 in
R3(config-if)#exit
```

5、配置完成后，在 R4 上确认 ACL 的配置结果：

```
R4#telnet 64.35.136.10

Trying 64.35.136.10 ...
% Destination unreachable; gateway or host down

R4#telnet 64.35.136.20

Trying 64.35.136.20 ...
% Destination unreachable; gateway or host down

R4#ping 64.35.136.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.35.136.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R4#
```

批注 [stanley794]：此时 R4 已无法访问内部网络。

批注 [stanley795]：ICMP 的数据包也无法到达内网。

6、在 R1 或 R2 上测试对外网的访问：

```
R1#ping 202.102.48.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

批注 [stanley796]：虽然 ACL 有效保护了内网的安全。但同时内网的主机也无法访问外网。

```
R2#telnet 202.102.48.1
Trying 202.102.48.1 ...
% Connection timed out; remote host not responding

R2#
```

批注 [stanley797]：R2 也无法对外网实施访问。

7、经过测试发现，R4 虽然已经无法访问内部网络。但是 R1 和 R2 也无法访问外部网络。**产生此问题的原因是因为 ACL 其拒绝了外网向内部网络的数据包发送。**

而 ICMP 和 TELNET 都会有回复的数据包，由于 ACL 的拒绝所有的配置，导致了回复数据包也无法返回到内部网络。

8、为了解决这一问题，可以在 R3 上实施 RACL 即反射 ACL 配置：

```
R3(config)#no access-list 1
R3(config)#
R3(config)#interface serial 1/1
R3(config-if)#no ip access-group 1 in
R3(config-if)#exit
R3(config)#
R3(config)#ip access-list extended in2out
R3(config-ext-nacl)#permit tcp any any eq telnet reflect tcp_racl
R3(config-ext-nacl)#permit icmp any any reflect icmp_racl
R3(config-ext-nacl)#exit
R3(config)#ip access-list extended out2in
R3(config-ext-nacl)#
R3(config-ext-nacl)#evaluate tcp_racl
R3(config-ext-nacl)#evaluate icmp_racl
R3(config-ext-nacl)#deny ip any any
R3(config-ext-nacl)#exit
R3(config)#
```

批注 [stanley798]：构建一个扩展的名称 ACL，并命名为 in2OUT，本 ACL 的主要目的是，标识出内部到外部的流量。

批注 [stanley799]：如果内网到外网有 TELNET 的访问，则为其创建反射的 ACL 条目，放入到外部的接口的 IN 的方向上允许数据包的返回。

Reflect 是指在指定的 RACL 中建立条目。其主要使用是分类动态创建的反射 ACL，以便于排错。

9、将 RACL 配置到接口：

```
R3(config)#interface serial 1/1
R3(config-if)#ip access-group in2out out
R3(config-if)#ip access-group out2in in
R3(config-if)#exit
```

批注 [stanley800]：引用之前配置 RACL 的 tcp_racl 的条目，并为其所指出的流量，动态的创建反射 ACL。

10、查看 R3 的 access-lists 的配置：

```
R3#show ip access-lists
Reflexive IP access list icmp_racl
Extended IP access list in2out
    10 permit icmp any any reflect icmp_racl (9 matches)
    20 permit tcp any any eq telnet reflect tcp_racl (24 matches)
Extended IP access list out2in
    20 evaluate tcp_racl
    30 deny ip any any (25 matches)
Reflexive IP access list tcp_racl
R3#
```

批注 [stanley801]：由于此时，并没有实际流量。因此并没有任何的反射 ACL 被创建。

批注 [stanley802]：由于此时，并没有实际流量。因此并没有任何的反射 ACL 被创建。

11、在 R4 上测试 RACL 的配置：

```
R4#
R4#ping 64.35.136.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.35.136.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R4#
R4#telnet 64.35.136.10
Trying 64.35.136.10 ...
% Destination unreachable; gateway or host down
R4#
```

批注 [stanley803]：此时外网仍然无法访问内网的主机。

12、观察 R3 的 access-lists：

```
R3#show ip access-lists
Reflexive IP access list icmp_racl
Extended IP access list in2out
    10 permit icmp any any reflect icmp_racl (9 matches)
    20 permit tcp any any eq telnet reflect tcp_racl (24 matches)
Extended IP access list out2in
    20 evaluate tcp_racl
    30 deny ip any any (25 matches)
Reflexive IP access list tcp_rReflexive IP access list tcp_racl
R3#
```

批注 [stanley804]：没有任何的 RACL 被创建。

批注 [stanley805]：没有任何的 RACL 被创建。

13、在 R1 或 R2 上测试：

```
R1#telnet 202.102.48.1
Trying 202.102.48.1 ... Open
User Access Verification
Password:
R4>
R4>
R4>logout
[Connection to 202.102.48.1 closed by foreign host]
R1#
R1#ping 202.102.48.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/136/192 ms
R1#
```

```
R2#telnet 202.102.48.1

Trying 202.102.48.1 ... Open
User Access Verification
Password: ******
R4>
```

批注 [stanley806]：可以成功的由内网向外网发起 TELNET 的连接。

批注 [stanley807]：退出远程 Telnet。

```
R4>logout
[Connection to 202.102.48.1 closed by foreign host]
R2#
R2#ping 202.102.48.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/190/232 ms
R2#
```

14、查看 R3 的 access-list 信息：

```
R3#show ip access-lists
Reflexive IP access list icmp_racl
     permit icmp host 202.102.48.1 host 64.35.136.20  (9 matches) (time left 285)
     permit icmp host 202.102.48.1 host 64.35.136.10  (29 matches) (time left 298)
Extended IP access list in2out
    10 permit icmp any any reflect icmp_racl (47 matches)
    20 permit tcp any any eq telnet reflect tcp_racl (148 matches)
Extended IP access list out2in
    10 permit icmp any any echo-reply (25 matches)
    20 evaluate tcp_racl
    30 deny ip any any (28 matches)
Reflexive IP access list tcp_racl
    permit tcp host 202.102.48.1 eq telnet host 64.35.136.10 eq 19787 (65 matches) (time left
0)
     permit tcp host 202.102.48.141 eq telnet host 64.35.136.10 eq 12412 (1 match) (time left
228)
R3#
```

批注 [stanley808]： 为 icmp 协议动态创建反射 ACL。其允许了外网主机到内网主机的 ICMP 的协议。

Time left 指出，被创建的反射 ACL 可以存活多久。

批注 [stanley809]： 为 TCP 协议创建的反射 ACL。其允许外网主机到内网主机的相应的 TCP 的流量。

15、由于默认情况下针对所有协议会话的反射 ACL 的存活时间为 300 秒。而对于 ICMP 或是 UDP 来说，其会话一般会在 1 到 5 秒内完成。如果反射 ACL 的存活时间过长，则暴露给 Dos 或是其他类型的攻击的可能性就更大。因此，强烈建议为无连接的会话改变默认会话值。示例如下：

```
R3(config)#ip access-list extended in2out
R3(config-ext-nacl)#permit icmp any any reflect icmp_racl timeout 10
R3(config-ext-nacl)#permit tcp any any eq telnet reflect tcp_racl
R3(config-ext-nacl)#permit udp any any reflect udp_racl timeout 10
R3(config-ext-nacl)#end
```

批注 [stanley810]： 指定 ICMP 的会话时间为 10 秒。即动态创建 RACL 的存活时间为 10 秒。

16、再次在 R1 上使用 ping 测试指定的会话时间值：

```
R1#ping 202.102.48.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/169/264 ms
R1#
```

17、查看 R3 的 access-lists 信息：

```
R3#show ip access-lists
Reflexive IP access list icmp_racl
     permit icmp host 202.102.48.1 host 64.35.136.10  (9 matches) (time left 8)
Extended IP access list in2out
    10 permit icmp any any reflect icmp_racl (18 matches)
    20 permit tcp any any eq telnet reflect tcp_racl
    30 permit udp any any reflect udp_racl
Extended IP access list out2in
    20 evaluate tcp_racl
    30 deny ip any any (37 matches)
Reflexive IP access list tcp_racl
Reflexive IP access list udp_racl
R3#
```

批注 [stanley811]: 针对 ICMP 创建的 RACL 的存活时间为 10 秒。由于无法在发出第一个 PING 同时，即获取 access-list 信息。因此此外显示为 8 秒。

18、实验完成。

CCNP Lab Manual

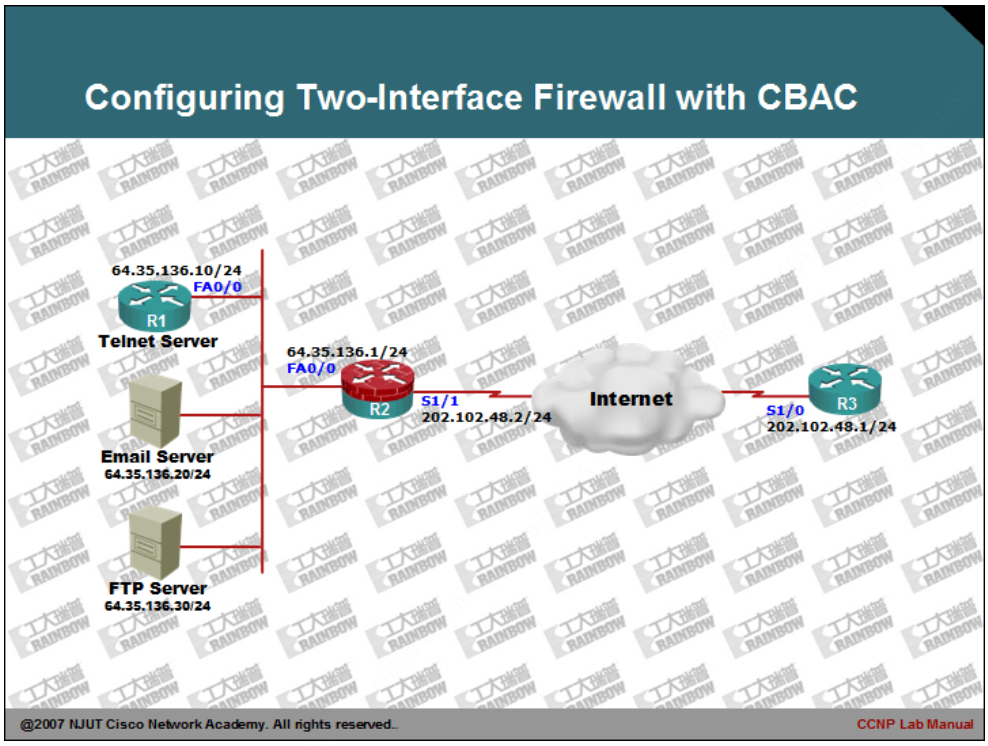
Lab 69. Configuring Two-Interface Firewall with CBAC

实验目的：

1、掌握 CBAC 基于上下文的访问控制列表配置方法。

2、理解 CBAC 的工作原理。

实验拓扑图：



实验步骤及要求：

1、实验拓扑中的 FTP 与 EMAIL 服务器，请自行搭建，本实验仅给出如何对 EMAIL 与 FTP 的服务的流量进行检测的配置。

2、本实验中，放置各种服务器的网络应被称为“受保护的网络”，为了方便叙述本文均称为“内网”与“外网”。

3、配置各台路由器的 IP 地址，并且使用 ping 命令确认各路由器的直连口的互通性。

4、配置 R1 路由器为 Telnet Server 服务器：

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

5、在 R1 配置静态路由，指向默认网关：

```
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 64.35.136.1
R1(config)#
```

6、配置 R3 路由器静态路由，确保数据包可以返回本地网络：

```
R3(config)#
R3(config)#ip route 64.35.136.0 255.255.255.0 202.102.48.2
R3(config)#
```

7、在 R1 和 R3 测试是否可以相互通讯，如果已配置好 FTP 和 EMAIL 服务器，请同时测试 FTP 是否可以登录，以及是否可以利用 EMAIL 收发邮件，下面仅给出 Telnet 与 ICMP 的测试结果：

```
R3#ping 64.35.136.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.35.136.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/61/100 ms
R3#
R3#telnet 64.35.136.10
Trying 64.35.136.10 ... Open
User Access Verification
Password:
R1>logout

[Connection to 64.35.136.10 closed by foreign host]
```

```
R3#
```

R1 的测试如下：

```
R1#
R1#telnet 202.102.48.1
Trying 202.102.48.1 ... Open

User Access Verification

Password:
R3>logout

[Connection to 202.102.48.1 closed by foreign host]
R1#
R1#ping 202.102.48.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/57/84 ms
R1#
```

8、通过以上的测试，可以看出，此时内外网均可以相互的通讯。

9、为了确保内部网络的安全，需要对某些进行了审查。例如仅允许源自于内部网络会话流量，访问内部网络，而禁止发起于外部网络的流量直接进入内部网络。除了可以配置 RACL 实现以外，也可以使用 CBAC 的配置实现。

10、首先在 R2 上 ACL，允许外出的会话流量，同时拒绝外网的向内网的访问，并且将配置好的 ACL 应用到接口上：

```
R2(config)#ip access-list extended inside_acl
R2(config-ext-nacl)#permit icmp any any
R2(config-ext-nacl)#permit tcp any any
R2(config-ext-nacl)#permit udp any any
R2(config-ext-nacl)#exit
R2(config)#
R2(config)#ip access-list extended outside_acl
R2(config-ext-nacl)#permit tcp any host 64.35.136.20 eq smtp
R2(config-ext-nacl)#permit tcp any host 64.35.136.30 eq ftp
R2(config-ext-nacl)#
R2(config-ext-nacl)#deny ip any any log
R2(config-ext-nacl)#exit
R2(config)#
R2(config)#interface fastEthernet 0/0
```

批注 [stanley812]： 允许外网的到 SMTP 和 FTP 的访问。但是需要注意的是 FTP 路由器如果仅这样配置，可能会无法访问。具体原因，是因为 FTP 的被动或是主动模式协商过程导致的。

批注 [stanley813]： log 的参数主要目的是：使 IOS 将符合条件的匹配记录到打开的日志记录设备。
如果没有配置日志记录设备，则直接显示在 IOS 的控制台窗口中。此命令会严重影响 IOS 的性能。

```
R2(config-if)#ip access-group inside_acl in
R2(config-if)#exit
R2(config)#
R2(config)#interface serial 1/1
R2(config-if)#ip access-group outside_acl in
R2(config-if)#exit
R2(config)#
```

11、关于 LOG 性能的影响问题，可以使用如下命令降低对 IOS 的性能影响：

```
R2(config)#ip access-list log-update threshold 10
```

批注 [stanley814]：配置当匹配 10 后，产生一个日志信息。

12、当配置完 ACL 后，在 R1 和 R3 上测试结果如下，可以看出此时不管是内网还是外网：

```
R1#ping 202.102.48.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

```
R3#ping 64.35.136.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.35.136.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R3#
```

13、配置 R2 的 CBAC，开启对相应的协议的审查：

```
R2(config)#ip inspect name myCBAC smtp
R2(config)#ip inspect name myCBAC ftp
R2(config)#ip inspect name myCBAC icmp timeout 10
R2(config)#ip inspect name myCBAC telnet
R2(config)#
R3(config)#ip inspect tcp idle-time 300
R2(config)#
R3(config)#ip inspect tcp synwait-time 30
R3(config)#
R3(config)#ip inspect tcp finwait-time 5
R3(config)#
R3(config)#ip inspect udp idle-time 30
R3(config)#
R3(config)#ip inspect dns-timeout 5
```

批注 [stanley815]：需要注意的是 CBAC 对 SMTP 的审查不支持 ESMTP。如果内部使用 SMTP 服务器，请关闭对 SMTP 的流量的审查。

批注 [stanley816]：指定 ICMP 的会话超时时间。

批注 [stanley817]：将 TCP 的连接空闲定时器从默认的 3600 秒修改为 300 秒。能够快速的收敛状态表，减少被攻击的可能。

批注 [stanley818]：配置 TCP 的三次握手时间，默认为 30 秒。以防止半开的 Dos 的攻击。

批注 [stanley819]：配置 TCP 的断开连接的时间，默认为 5 秒。

批注 [stanley820]：配置 UDP 的会话超时时间。

批注 [stanley821]：配置 DNS 的查询超时时间，默认为 5 秒。用来来阻止黑客的 DNS 回复欺骗。

```
R3(config)#
R2(config)#interface serial 1/1
R2(config-if)#ip inspect myCBAC out
R2(config-if)#exit
R2(config)#
R3(config)#ip inspect hashtable-size 1024
R3(config)#
```

批注 [stanley822]：对外出的流量进行审查。

批注 [stanley823]：配置 CBAC 吞吐量特性。CBAC 会为每个会话生成一个 HASH 值存入状态表。以便于使用快速查找会话信息。如果路由器遇到会话较多时，可以调整此 HASH 漏桶数量。
默认为 1024。而且此数量近似与会话总量。

14、配置完成后，在 R3 路由器上，使用 ping 和 telnet 命令继续测试，如果存在 EMAIL 和 FTP 服务器。请自行测试。测试结果如下：

```
R3#telnet 64.35.136.10
Trying 64.35.136.10 ...
% Destination unreachable; gateway or host down

R3#ping 64.35.136.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.35.136.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R3#
```

在 R2 路由器上，可以注意到 IOS 提示的数据包被拦截的信息：

```
*Jul 14 17:39:14.487: %SEC-6-IPACCESSLOGDP: list outside_acl denied icmp 202.102.48.1 ->
64.35.136.10 (0/0), 1 packet
*Jul 14 17:40:22.787: %SEC-6-IPACCESSLOGP: list outside_acl denied tcp 202.102.48.1(0) ->
64.35.136.10(0), 1 packet
```

15、回到 R1 上，使用 ping 和 telnet 测试对外网的访问：

```
R1#ping 202.102.48.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/66/104 ms
R1#
R1#telnet 202.102.48.1
Trying 202.102.48.1 ... Open
User Access Verification

Password:
R3>
R3>logout

[Connection to 202.102.48.1 closed by foreign host]
```

```
R1#
```

16、在 R2 路由器，查看 CBAC 检测的会话信息：

```
R2#show ip inspect sessions
Established Sessions
 Session 65F31950 (64.35.136.10:24367)=>(202.102.48.1:23) telnet SIS_OPEN
R2#
R2#show ip inspect all
.........
Interface Configuration
 Interface Serial1/1
  Inbound inspection rule is not set
  Outgoing inspection rule is myCBAC
    smtp max-data 20000000 alert is on audit-trail is off timeout 3600
    ftp alert is on audit-trail is off timeout 3600
    icmp alert is on audit-trail is off timeout 10
    telnet alert is on audit-trail is off timeout 3600
    pop3 alert is on audit-trail is off timeout 3600
  Inbound access list is outside_acl
  Outgoing access list is not set

Established Sessions
 Session 65F31950 (64.35.136.10:53198)=>(202.102.48.1:23) telnet SIS_OPEN
R2#
```

批注 [stanley824]: CBAC 检测到的会话信息及状态。

17、R2 上查看 CBAC 的配置信息：

```
R2#show ip inspect name myCBAC
Inspection name myCBAC
    smtp max-data 20000000 alert is on audit-trail is off timeout 3600
    ftp alert is on audit-trail is off timeout 3600
    icmp alert is on audit-trail is off timeout 10
    telnet alert is on audit-trail is off timeout 3600
    pop3 alert is on audit-trail is off timeout 3600
```

18、还可以使用如下命令查看 CBAC 的一些信息，具体不在列出：

```
R2#show ip inspect ?
  all         Inspection all available information
  config      Inspection configuration
  ha          Show commands for IOS firewalli High Availability
  interfaces  Inspection interfaces
  mib         FW MIB specific show commands
  name        Inspection name
  sessions    Inspection sessions
  statistics  Inspection statistics
```

19、实验完成。

http://cisco.njut.edu.

CCNP Lab Manual

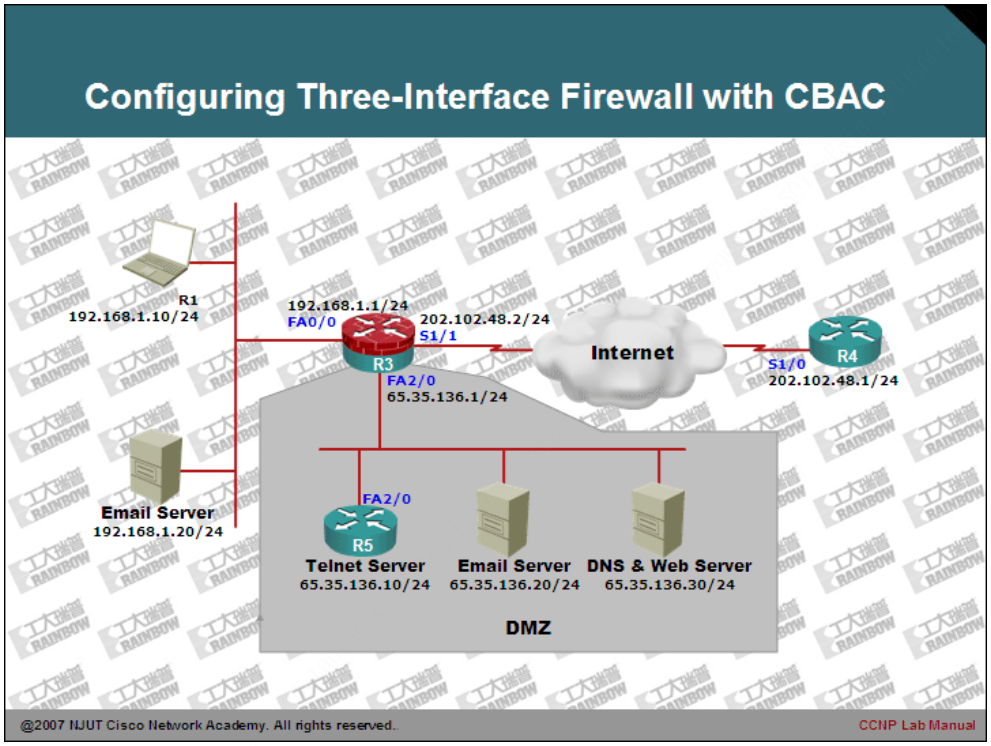
Lab 70. Configuring Three-Interface Firewall with CBAC

实验目的：

1、掌握 CBAC 基于上下文的访问控制列表配置方法。

2、理解 CBAC 的工作原理。

实验拓扑图：



实验步骤及要求：

1、配置各路由器 IP 地址，并且使用 ping 命令确认直接路由器的连接。请各位自己配置 Email 服务器用于测试 CBAC。本实验不包含 EMAIL 和 WEB 以及 DNS 服务器的配置和测试结果，仅给出相应的 CBAC 的配置命令。

2、首先使用 ping 命令测试目前网络的通讯：

```
R1#ping 65.35.136.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 65.35.136.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/61/80 ms
R1#
R1#telnet 65.35.136.10
Trying 65.35.136.10 ... Open

User Access Verification

Password:
R5>
R5>logout

[Connection to 65.35.136.10 closed by foreign host]
R1#
R1#ping 202.102.48.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/74/100 ms
R1#
R1#telnet 202.102.48.1
Trying 202.102.48.1 ... Open
User Access Verification
Password:

R4>logout

[Connection to 202.102.48.1 closed by foreign host]
R1#
```

批注 [stanley825]： R1 可以 ping 通 DMZ 区域的 Telnet 服务器。

批注 [stanley826]： R1 路由器同时也可以使用 telnet 命令访问 DMZ 区域的 Telnet 服务器。

批注 [stanley827]： R1 也可以使用 ping 访问 R4 路由器。

批注 [stanley828]： 测试到外网的 Telnet 连接。

批注 [stanley829]： 通过主机名看出，R1 可以登录到外网路由器。

而对于 R5 路由器和 R4 路由器，此时也是可以相互访问，并没有任何限制，详细

结果不在列出。

3、**本实验的需求如下**：

1) Internet 能够访问 DMZ 区域的 Email，WEB 和 Telnet 服务器。

2) Internet 不允许访问内部网络，即 192.168.1.0/24 的子网。

3) 内部网主机仅能够向 DMZ 区域的 DNS 进行域名的解析查询。

4) 内部 Email 服务器只能访问 DMZ 区域的 Email 服务器。

5) 内部用户能够访问 Internet 网络和接收回复。

6) 内部用户可以访问 DMZ 区域的 Telnet 服务器，并且仅限 Telnet 方式。

7) 内部用户服务仅能访问内部网络的 Email 服务器收发邮件。

8) DMZ 区域 Email 的服务器能够访问内部的 Email 服务器转发邮件。

4、配置 R2 路由器的 CBAC，实施 IOS 的防火墙特性。

5、首先配置针对内部网络的 CBAC 和 ACL 条目，配置如下：

```
R3(config)#ip access-list extended inside_acl
R3(config-ext-nacl)#5 permit tcp any host 65.35.136.30 eq domain
R3(config-ext-nacl)#6 permit udp any host 65.35.136.30 eq domain
R3(config-ext-nacl)#
R3(config-ext-nacl)#permit tcp host 192.168.1.20 host 65.35.136.20 eq smtp
R3(config-ext-nacl)#
R3(config-ext-nacl)#permit tcp any host 65.35.136.10 eq telnet
R3(config-ext-nacl)#deny ip any host 65.35.136.10
R3(config-ext-nacl)#
R3(config-ext-nacl)#deny tcp any any eq pop3
R3(config-ext-nacl)#deny tcp any any eq smtp
R3(config-ext-nacl)#
R3(config-ext-nacl)#permit ip any any
R3(config-ext-nacl)#exit
R3(config)#
R3(config)#ip inspect name inside_CBAC smtp
R3(config)#ip inspect name inside_CBAC ftp
R3(config)#ip inspect name inside_CBAC http
R3(config)#ip inspect name inside_CBAC tcp
R3(config)#ip inspect name inside_CBAC udp
R3(config)#ip inspect name inside_CBAC icmp timeout 5
R3(config)#ip inspect name inside_CBAC dns
R3(config)#
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip access-group inside_acl in
```

批注 [stanley830]： 内网主机到 DMZ 区域的 DNS 的域名查询解析。

批注 [stanley831]： 允许内网的 Email 到 DMZ 的 Email 的通信。

批注 [stanley832]： 允许内网主机到 DMZ 区域 Telnet 服务器的访问。

批注 [stanley833]： 拒绝内网主机到 DMZ 区域的 Telnet 服务器其它方式的访问。

批注 [stanley834]： 拒绝内网主机到任何非内部网络的 Email 服务器的访问。

批注 [stanley835]： 允许其它的安全数据流量。

批注 [stanley836]： 针对 ICMP 的无状态的访问设置其 5 秒的会话超时。

```
R3(config-if)#ip inspect inside_CBAC in
R3(config-if)#exit
R3(config)#
```

6、配置针对 DMZ 区域的 CBAC 和 ACL：

```
R3(config)#ip access-list extended dmz_acl
R3(config-ext-nacl)#permit tcp host 65.35.136.20 any eq smtp
R3(config-ext-nacl)#
R3(config-ext-nacl)#permit udp host 65.35.136.30 any eq domain
R3(config-ext-nacl)#permit tcp host 65.35.136.30 any eq domain
R3(config-ext-nacl)#exit
R3(config)#
R3(config)#
R3(config)#ip inspect name dmz_CBAC smtp
R3(config)#ip inspect name dmz_CBAC tcp
R3(config)#ip inspect name dmz_CBAC udp
R3(config)#ip inspect name dmz_CBAC dns
R3(config)#
R3(config)#interface fastEthernet 2/0
R3(config-if)#ip access-group dmz_acl in
R3(config-if)#ip inspect dmz_CBAC in
R3(config-if)#exit
R3(config)#
```

批注 [stanley837]：允许 DMZ 区域的邮件服务器与 Internet 上的其它 Email 的服务器进行邮件的转发。

批注 [stanley838]：配置允许 DMZ 区域 DNS 向 Internet 网络发起域名查询。配置此条目，主要目的是，DNS 可能会向根服务器或上级 DNS 服务器发起域名解析的请求。

7、配置针对 Internet 区域的 CBAC 和 ACL 的条目：

```
R3(config)#ip access-list extended outside_acl
R3(config-ext-nacl)#permit tcp any host 65.35.136.10 eq telnet
R3(config-ext-nacl)#permit tcp any host 65.35.136.30 eq www
R3(config-ext-nacl)#permit tcp any host 65.35.136.30 eq smtp
R3(config-ext-nacl)#exit
R3(config)#
R3(config)#ip inspect name outside_CBAC http
R3(config)#ip inspect name outside_CBAC dns
R3(config)#ip inspect name outside_CBAC smtp
R3(config)#ip inspect name outside_CBAC tcp
R3(config)#ip inspect name outside_CBAC udp
R3(config)#ip inspect name outside_CBAC icmp timeout 5
R3(config)#
R3(config)#interface serial 1/1
R3(config-if)#ip access-group outside_acl in
R3(config-if)#ip inspect outside_CBAC in
R3(config-if)#exit
R3(config)#
```

8、为了确保网络的安全，建议同时在 R3 路由器上配置如下命令：

```
R3(config)#
R3(config)#ip inspect dns-timeout 5
R3(config)#ip inspect tcp idle-time 300
R3(config)#ip inspect tcp synwait-time 30
R3(config)#ip inspect udp idle-time 20
R3(config)#
```

批注 [stanley839]: 配置 DNS 的查询超时时间为 5 秒。

9、在 R1、R5 和 R4 上测试 CBAC，关于 Email、WEB、DNS 的测试，请根据各位自己搭建的实验环境完成测试。本实验仅实验简单的测试：

```
R4#ping 65.35.136.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 65.35.136.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R4#
R4#
R4#telnet 65.35.136.10
Trying 65.35.136.10 ... Open

User Access Verification

Password:
Password:
R5>
R5>
R5>logout

[Connection to 65.35.136.10 closed by foreign host]
R4#
R4#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R4#
R4#
```

批注 [stanley840]: 外网无法使用 ICMP 协议访问 DMZ 区域主机。

批注 [stanley841]: 向 DMZ 区域进行 Telnet 连接。

批注 [stanley842]: Telnet 的连接可以正常的访问。

批注 [stanley843]: 外网无法使用 ICMP 协议访问内网。

路由器 R5 的测试结果：

```
R5#ping 202.102.48.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
```

```
U.U.U
Success rate is 0 percent (0/5)
R5#
R5#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R5#
R5#telnet 202.102.48.1
Trying 202.102.48.1 ...
% Destination unreachable; gateway or host down

R5#telnet 192.168.1.10
Trying 192.168.1.10 ...
% Destination unreachable; gateway or host down

R5#
```

在路由器 R1 的测试结果：

```
R1#ping 202.102.48.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.102.48.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/74/100 ms
R1#
R1#telnet 202.102.48.1
Trying 202.102.48.1 ... Open
User Access Verification
Password:
R4>logout
[Connection to 202.102.48.1 closed by foreign host]
R1#
R1#telnet 65.35.136.10
Trying 65.35.136.10 ... Open
User Access Verification

Password:
R5>
R5>
R5>logout

[Connection to 65.35.136.10 closed by foreign host]
```

批注 [stanley844]: 内网到外网的 ICMP 的访问。

批注 [stanley845]: 内网到外网的 Telnet 的访问。

批注 [stanley846]: 内网到 DMZ 区域的 telnet 访问。

```
R1#
R1#
R1#ping 65.35.136.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 65.35.136.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
R1#
```

批注 [stanley847]: 内网到 DMZ 区域的 icmp 的访问，被成功的拒绝。

10、还可以使用下面的命令查看 CBAC 的状态信息，请自己行测试：

```
R2#show ip inspect ?
  all         Inspection all available information
  config      Inspection configuration
  ha          Show commands for IOS firewalli High Availability
  interfaces  Inspection interfaces
  mib         FW MIB specific show commands
  name        Inspection name
  sessions    Inspection sessions
  statistics  Inspection statistics
```

11、实验完成。

CCNP Lab Manual

Lab 71. Configuring Cisco Router AutoSecure

实验目的：

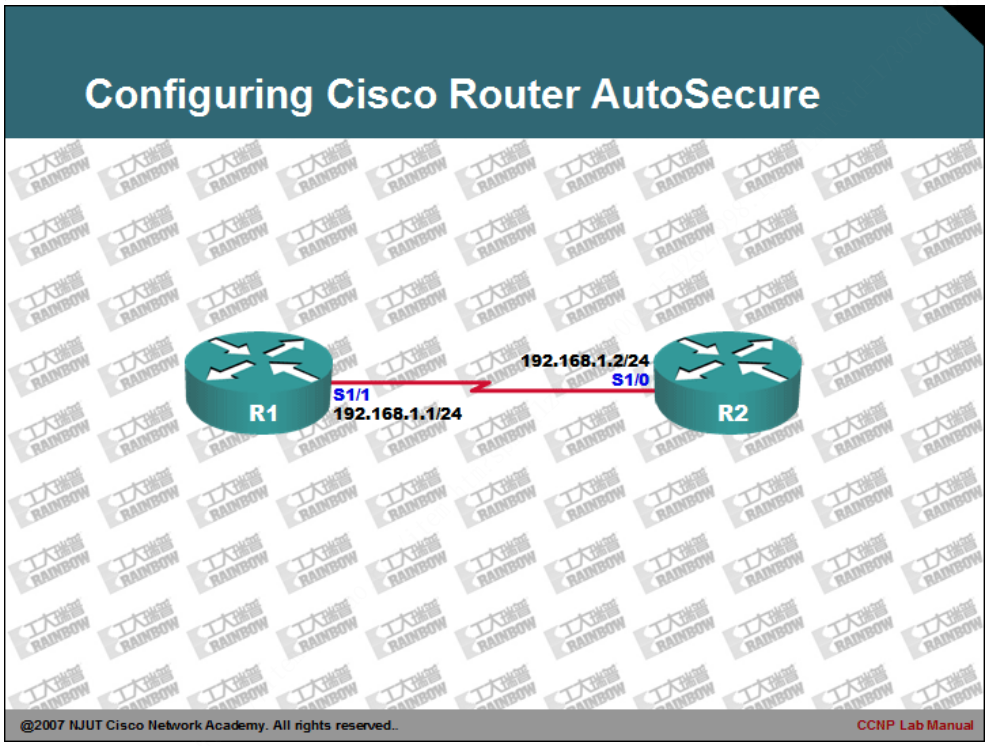
1、利用 Cisco 路由器的 AutoSecure 功能，关闭所有可能被黑客利用的服务及漏洞。

2、AutoSecure 存有两模式：a.交互模式 b.非交互模式。

3、确认 AutoSecure 配置。

4、AutoSecure 运行在 Cisco IOS 12.2(18)和 12.3(1)或之后版本中。

实验拓扑图：



实验步骤及要求：

1、配置 R1 和 R2 路由器的 IP，同时配置 R1 路由器的 Telnet 服务。并在 R2 路由器向 R1 发起 telnet 的访问，确认配置：

```
R2#telnet 192.168.1.1
Trying 192.168.1.1 ... Open

User Access Verification

Password:
R1>
R1>logout

[Connection to 192.168.1.1 closed by foreign host]
R2#
```

批注 [stanley848]：成功登录到 R1 路由器。

2、使用 AutoSecure 安全特征，配置路由器的安全。配置如下：

```
R1#auto secure
               --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

If this device is being managed by a network management station,
AutoSecure configuration may block network management traffic.
Continue with AutoSecure? [no]:yes
Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:Yes


Enter the number of interfaces facing the internet [1]:

Interface                  IP-Address      OK? Method Status                Protocol
```

批注 [stanley849]：通过 Auto secure 脚本命令进入交互式配置过程。

批注 [stanley850]：系统确认是否需要继续。此处，理所当然选择 yes。

批注 [stanley851]：系统询问此台路由器是否连接到 Internet。如果这是一台内部路由器，请选择 no。本例假设 R1 连接到 Internet 网络。

批注 [stanley852]：询问有多少个接口连接到 Internet。默认为 1。

```
FastEthernet0/0            unassigned      YES unset  administratively down down
Serial1/0                  unassigned      YES unset  administratively down down
Serial1/1                  192.168.1.1     YES manual up                    up
Serial1/2                  unassigned      YES unset  administratively down down
Serial1/3                  unassigned      YES unset  administratively down down
Serial2/0                  unassigned      YES unset  administratively down down
Serial2/1                  unassigned      YES unset  administratively down down
Serial2/2                  unassigned      YES unset  administratively down down
Serial2/3                  unassigned      YES unset  administratively down down
ATM3/0                     unassigned      YES unset  administratively down down
Enter the interface name that is facing the internet: FastEthernet0/0

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between
k and k, where k is any character}:
```

批注 [stanley853]： 填写连接到 Ineternet 网络的接口。

批注 [stanley854]： 系统开始配置管理层面的相关服务。
随后信息，是系统禁用了和启用部分的服务。

批注 [stanley855]： 配置一个简单的登录标识。类似于 banner motd。

```
* Warring
Unautorized access to this device is prohibited.
You must have explicit permission to access this
Device.
*

Enable secret is either not configured or
 is the same as the enable password
Enter the new enable secret:wangyuan
Confirm the enable secret :wangyuan

Enable password is not configured or its length
is less than minimum no. of characters configured
Enter the new enable password:stanley
Confirm the enable password:stanley

Configuration of local user database
Enter the username: wangyuan
Enter the password: cisco123
Confirm the password: cisco123

Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
to internet
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
```

批注 [stanley856]: 自定义的提示信息。

批注 [stanley857]: 配置加密级别的特权密码。

批注 [stanley858]: 同时系统还需要配置一个明文级的特权密码。

批注 [stanley859]: 配置一个存于本地认证数据库帐号条目，其将用于控制台和远程访问。

批注 [stanley860]: 自动配置 AAA。

```
be observed


Enable tcp intercept feature? [yes/no]: yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CUh6$W1CqOSONNeCJGj6jwBR6d.
enable password 7 0100120555070316
username wangyuan password 7 05070919244F5603
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
```

批注 [stanley861]： 系统访问是否开启 tcp 的拦截特性？

批注 [stanley862]： 下面为 auto secure 自动生成的配置命令。

```
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
int FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
int Serial1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int Serial1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int Serial1/2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int Serial1/3
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int Serial2/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int Serial2/1
 no ip redirects
```

```
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int Serial2/2
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int Serial2/3
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
int ATM3/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
ip cef
ip access-list extended 100
 permit udp any any eq bootpc
interface FastEthernet0/0
 ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end
Apply this configuration to running-config? [yes]:

Applying the config generated to running-config

R1#
```

批注 [stanley863]： 系统访问是否应用配置到 running-config 文件。

3、此时可以通过 show running-config 查看 AutoSecure 生成配置。也可以使用如下命令进行查看：

```
R1#show auto secure config
```

4、配置额外的选项，如下所示：

```
R1(config)#security passwords min-length 8
R1(config)#
R1(config)#
R1(config)#security authentication failure rate 3 log
R1(config)#
```

批注 [stanley864]：配置系统的密码长度最少为 8 位字符。

批注 [stanley865]：配置如果出现 3 次连续的失败认证的记录。系统默认将会暂停 15 秒，然后再接受新的处理请求。
系统默认值为：10 次。

需要注意的是：在不同的 IOS 版本，不仅可以指定配置认证失败的最大值，同时还可以修改默认的停止处理的周期。比如可以手工配置系统停止响应 30 分钟来增强安全性。同时也可以配置，完全开放的网络，即设置发起某个指定的网络的认证，即使出现多次失败，仍然不会对其停止响应。此源网络一般来自于授权的网管中心子网。

5、确认最小密码长度的配置：

```
R1(config)#username jear password cisco
% Password too short - must be at least 8 characters. Password configuration failed
```

批注 [stanley866]：由于配置密码长度小于指定的 8 位长度，因此，系统拒绝接受此帐号的配置。

6、在 R2 上使用 ping 和 telnet 测试 R1 的安全性：

```
R2#telnet 192.168.1.1
Trying 192.168.1.1 ... Open

Unautorized access to this device is prohibited.
You must have explicit permission to access this
Device.

User Access Verification

Username: wangyuan
Password: ********

R1>
```

批注 [stanley867]：自定义的 banner motd。

批注 [stanley868]：由于 auto secure 启用了 AAA。所以此处要求输入正确的帐号和密码。

批注 [stanley869]：根据提示符可以看出，成功的登录到 R1 路由器。

7、另外需要了解的是：auto secure 其安全配置依赖于 IOS 的版本，如果是一个带有 K9 的 IOS 版本，其还会询问您是否需要配置 SSH 的连接。SSH 的连接是基加密的一种类 telnet 的远程访问，其使用了不对称的密钥进行客户端的身份识别。同时还会默认开启对私有网络地址的拒绝。同时还会自动配置 Bogon 的过滤器。即对 IANA 机构未分配的 IP 地址进行过滤。这些地址通常会被黑客用于 DDos 的攻击。另外，还会访问是否需要配置单播逆向路径转发。同时也会访问是否需要配置 CBAC，当然此前提是您的 IOS 支持防火墙特性集的情况下才会发

生这个过程。

由于本实验中所使用的IOS并非带有防火墙特性集，因此无法观察到auto secure的更高级的配置。

8、实验完成。

CCNP Lab Manual

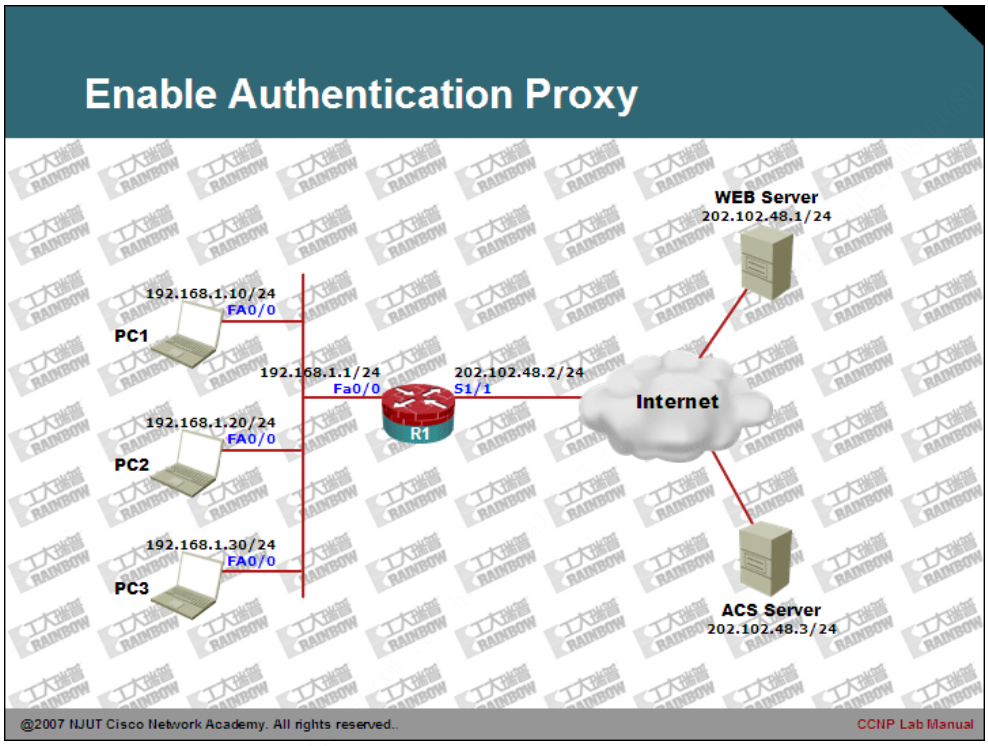
Lab 72. Enable Authentication Proxy

实验目的：

1、掌握 Cisco IOS 认证代理配置。

2、使用 TACACS+服务器配置用户帐号和密码。

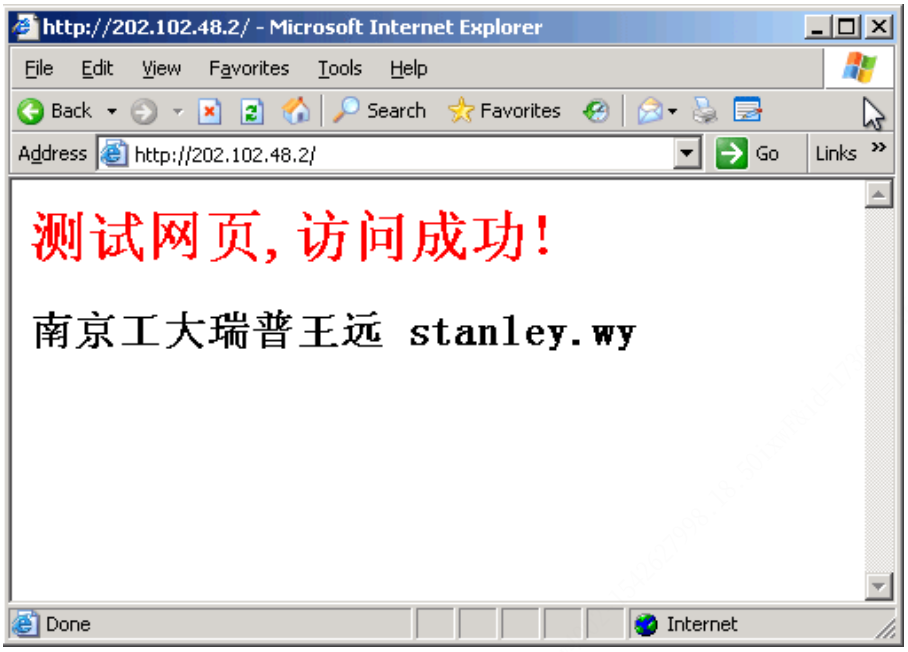
实验拓扑图：



实验步骤及要求：

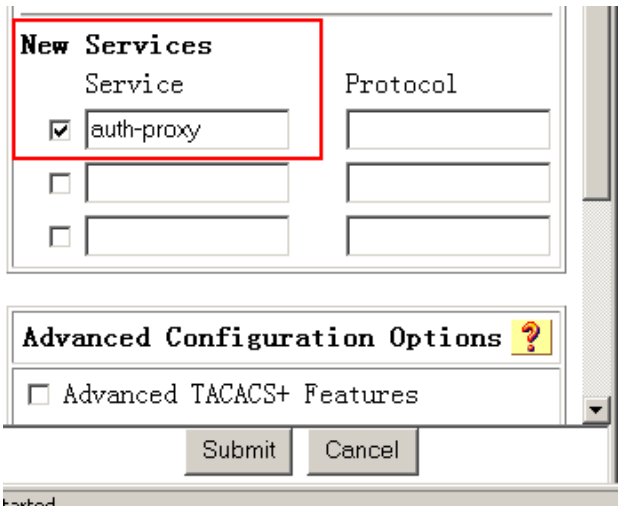
1、配置 R1 与 R2 路由器的 IP 地址，并且使用 ping 命令测试连接。同时配置 PC1、PC2、PC3 以及 ACS 服务器，确认其能够与 R1 路由器通讯。

2、在 PC1 上使用 IE 浏览器，浏览外部服务器进行测试，并确认可以正常访问 WEB 网页：



3、本实验中 ACS 的版本为 3.2 的版本，由于 AP 服务在 Cisco ACS 3.2 中默认是关闭的，因此需要配置 AAA 服务器，启用 AP 服务。

4、在 ACS 服务器的 WEB 管理窗口中，单击左侧边栏中的“Interface Configuration”按钮，在中间 WEB 页选择“TACACS+ (Cisco IOS)”连接。找到“TACACS+ Services”部分，在“New Service”下面，单击一个空的复选框，在“Service”栏下的文本框中，输入“auth-proxy”，单击窗口下面的“Submit”。如下面所示：



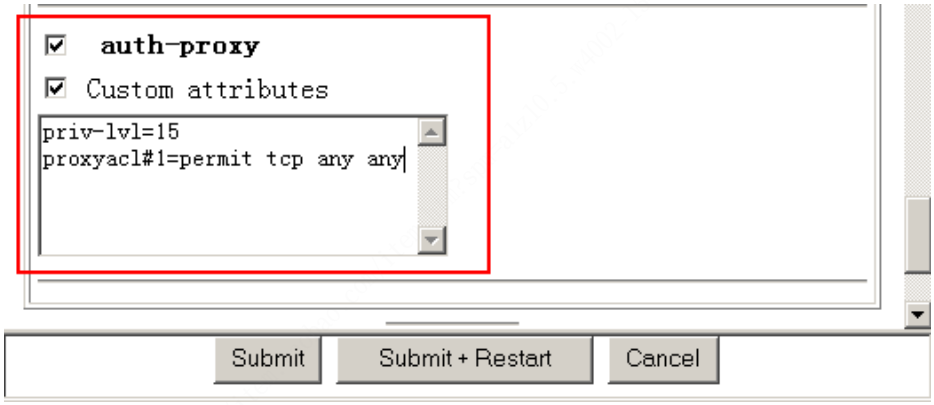
5、当启用 AP 服务后，需要在将其关联到组帐号。选择左边侧边栏的“Group Setup”，选择默认组并点击“Edit Settings”按钮，在随后的打开的页面中，寻找到之前启用“auth-proxy”在其前的复选框中打勾，同时在 Custom Attribute 的文本框中输入如下内容：

```
priv-lvl=15
proxyacl#1=permit tcp any any
```

批注 [stanley870]：配置认证后的权限，其必须是 15。Proxyacl#命令定论了 UAP（用户授权档案），其类似于 ACL。

需要注意的是第一个 any 为请必须使用关键字 any 不变，因此路由器从 ACS 接收到 UAP 后，会将源地址的 any 替换成认证用户实际的地址。

具体图示如下：



6、在 ACS 上创建一新用户 stanley，并从属于 default group。选择左边侧边栏的“User Setup”，在 user 关键字后的文本框中填写帐号名称，点击“Add/edit”按钮，在新开页面中，设置密码，同时保证其从属于 default group 组，点击页面最下方的 submit 按钮。

7、在路由器 R1 上配置 AAA：

```
R1(config)#aaa new-model
```

批注 [stanley871]：启用 AAA 认证模式。

```
R1(config)#
R1(config)#tacacs-server host 202.102.48.3 key cisco123
R1(config)#
R1(config)#aaa authentication login console none
R1(config)#
R1(config)#line console 0
R1(config-line)#login authentication console
R1(config-line)#exit
R1(config)#
R1(config)#aaa authentication login default group tacacs+
R1(config)#
R1(config)#aaa authorization auth-proxy default group tacacs+
R1(config)#
R1(config)#ip http server
R1(config)#
R1(config)#
R1(config)#ip http authentication aaa
R1(config)#
R1(config)#ip auth-proxy inactivity-timer 10
R1(config)#
R1(config)#ip auth-proxy name checkinside http
R1(config)#
R1(config)#
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip auth-proxy checkinside
R1(config-if)#exit
```

批注 [stanley872]：配置 AAA 服务器的地址，与连接密钥。

批注 [stanley873]：配置本地 console 登录不进行 AAA 的认证，主要避免 AAA 服务器出错，无法登录路由器控制台。

批注 [stanley874]：配置 console 口的认证方式。

批注 [stanley875]：启用 TACACS 的认证。

批注 [stanley876]：配置 TACACS 服务器打开 AP 授权。

批注 [stanley877]：配置 https 的认证采用 AAA 方式。

批注 [stanley878]：配置 AP 的缓存信息的空闲超为 10 分钟。默认为 60 分钟。其功能是，当用户过期后，路由器立即删除从 AAA 上下载的临时 ACL 的条目。

批注 [stanley879]：配置所有内部用户将会通过 HTTP 认证。

批注 [stanley880]：指定此接口使用 auth-proxy 进行身份认证。

8、在进行认证之前，先使用如下命令测试与 AAA 服务器通信：

```
R1#
R1#test aaa group tacacs+ stanley cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
R1#
```

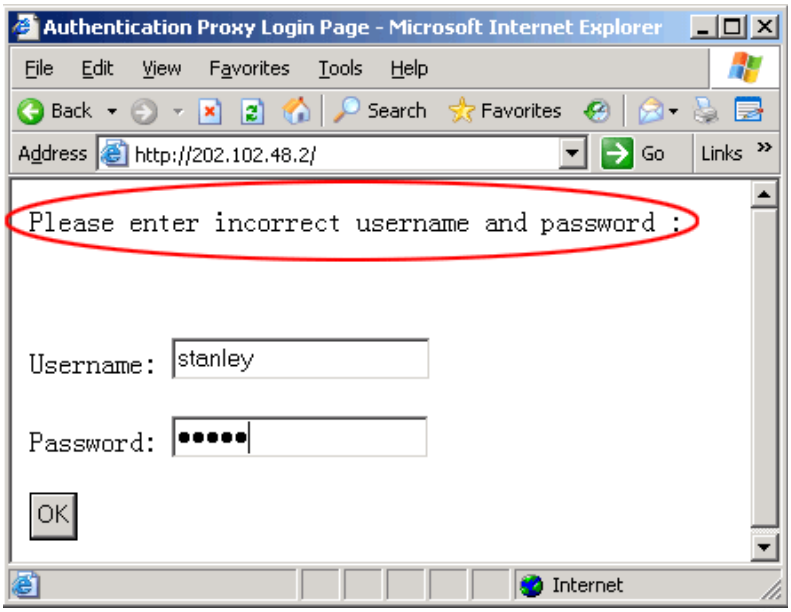
9、同时配置如下命令，以便于提供友好认证界面：

```
R1(config)#ip auth-proxy auth-proxy-banner http #
Enter TEXT message.  End with the character '#'.
Please enter incorrect username and password :
#
R1(config)#exit
```

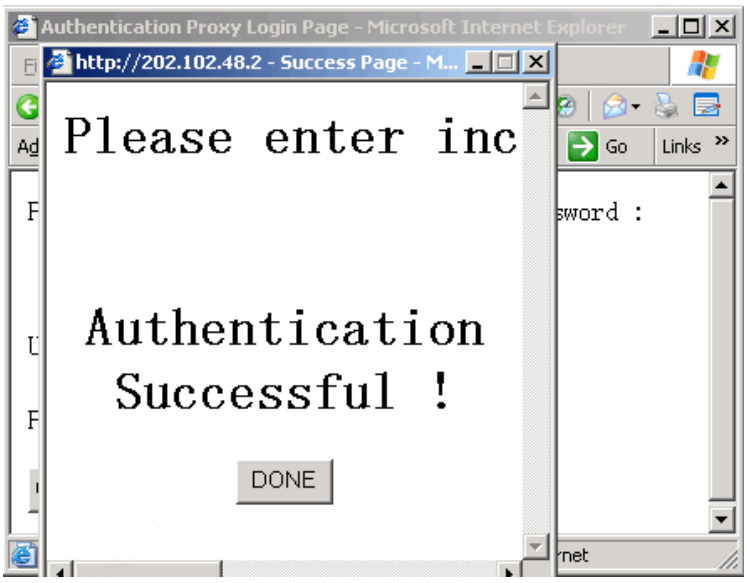
批注 [stanley881]：配置认证 banner 语句。

9、再次在 PC1 上使用 IE 浏览器浏览外部网络的 WEB 网页，进行测试，此时会发现，弹出的页面要求提供用户名和密码，填写在 TACACS+服务器上配置的用户帐

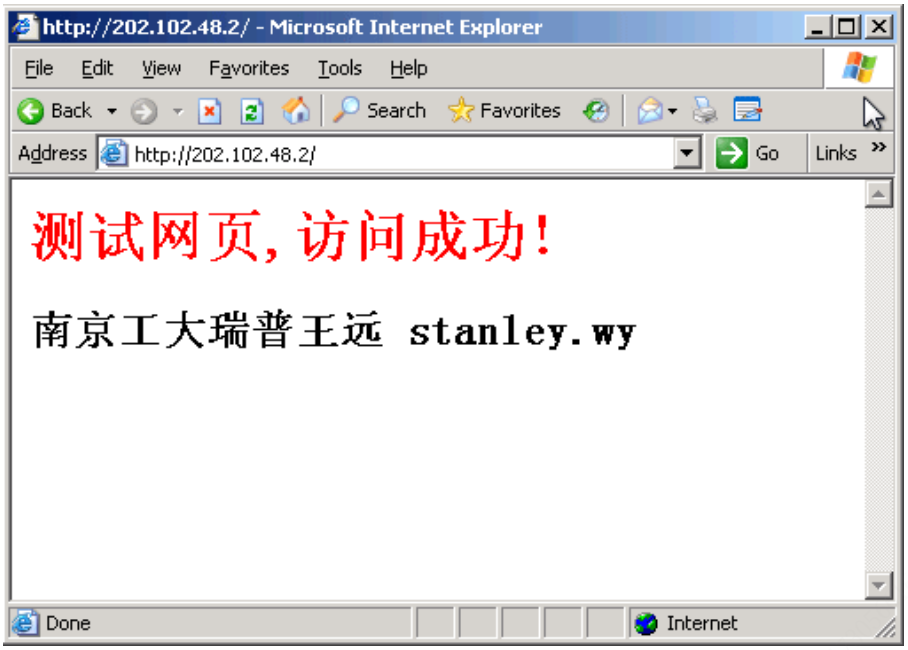
号和密码，点击 OK 按钮，进行认证：



10、如果一切配置正确的话，哪么将会出现如下认证成功的界面：



11、点击 DONE 的按钮，随后即可访问外部的 WEB 网站，如下图所示：



12、查看路由器的认证缓存：

```
R1#
R1#show ip auth-proxy cache
Authentication Proxy Cache
 Client Name stanley, Client IP 192.168.1.10, Port 1041, timeout 10, Time Remaining 10, state
ESTAB

R1#
```

13、实验完成。

CCNP Lab Manual

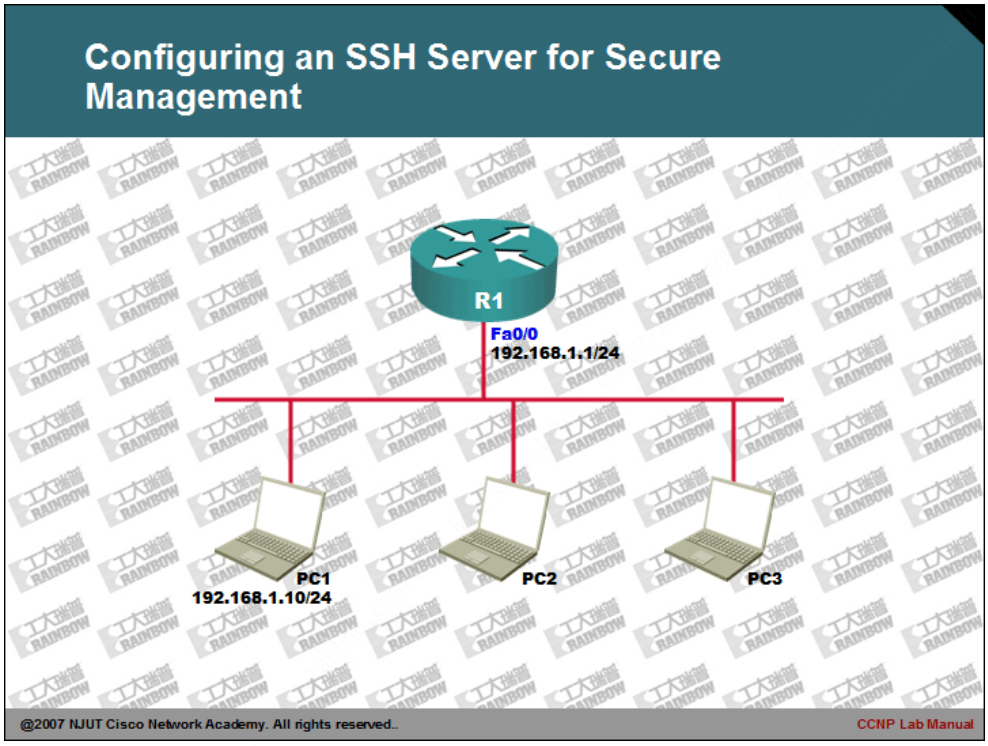
Lab 73. Configuring an SSH Server for Secure Management

实验目的：

1、掌握 SSH 配置方法。

2、使用 SSH 客户端软件连接到 SSH 路由器。

实验拓扑图：

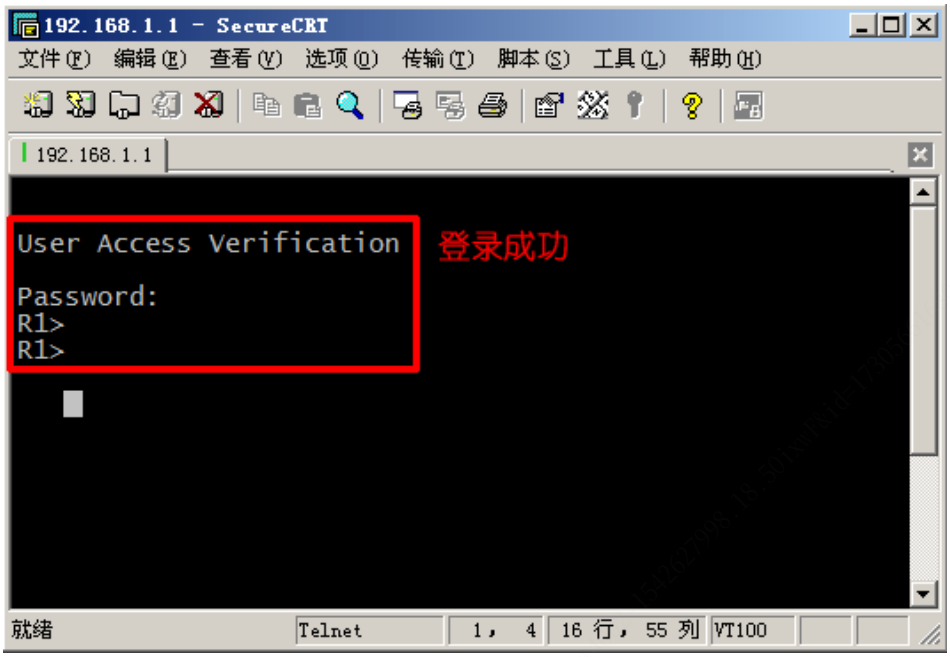


实验步骤及要求：

1、配置路由器与 PC 主机的 IP 地址，并且 ping 命令确认连接。

2、在 PC 主机上使用 telnet 软件连接到路由器 R1，本实验使用了 secureCRT 软件。

3、在 secureCRT 创建新的到达 R1 路由器的连接，并且尝试连接，确认结果：



4、此时使用的 Telnet 的连接方式，如果在网络安装有 sniffer 软件，则之前的 Telnet 密码可能已经被人截获。其主要原因是 telnet 发送的是明文密码。因此，有必须在路由器实施 SSH，SSH 连接使用了不对称钥的密码来与客户端协商认证，并且产生加密密钥，用于会话加密，有效的保护了 telnet 会话。

5、SSH 目前有两个版本，SSH1 使用 RSA 生成加密密钥。SSH2 则使用数字签名算法（DSA）密钥保护连接和认证。另外，我的同事崔北亮（CCIE16***）曾经提及 SSH2 是一个商业版本，使用时需要支付一定费用。因此，为了顺利完成本实验，决定不采用 SSH2，而采用 SSH1。

6、在 R1 路由器上配置 SSH 的服务器端，配置如下：

```
R1(config)#host R1
R1(config)#ip domain-name edurainbow.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.edurainbow.com
```

批注 [stanley882]：配置本地域名，用于生成证书。证书包含了公钥。

批注 [stanley883]：配置使用 RSA，生成一对密钥。

批注 [stanley884]：密钥的名称。

```
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
R1(config)#aaa new-model
R1(config)#
R1(config)#username wangyuan password cisco123
R1(config)#
R1(config)#ip ssh time-out 30
R1(config)#
R1(config)#
R1(config)#ip ssh authentication-retries 3
R1(config)#ip ssh time-out 120
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#end
R1(config)#
```

批注 [stanley885]：选择密钥的长度。默认为 512。

当前路由器的允许的范围是：
360 到 2048 位的长度。

批注 [stanley886]：配置 AAA 模式。

批注 [stanley887]：配置帐号和密码，用于 SSH 客户端登录。

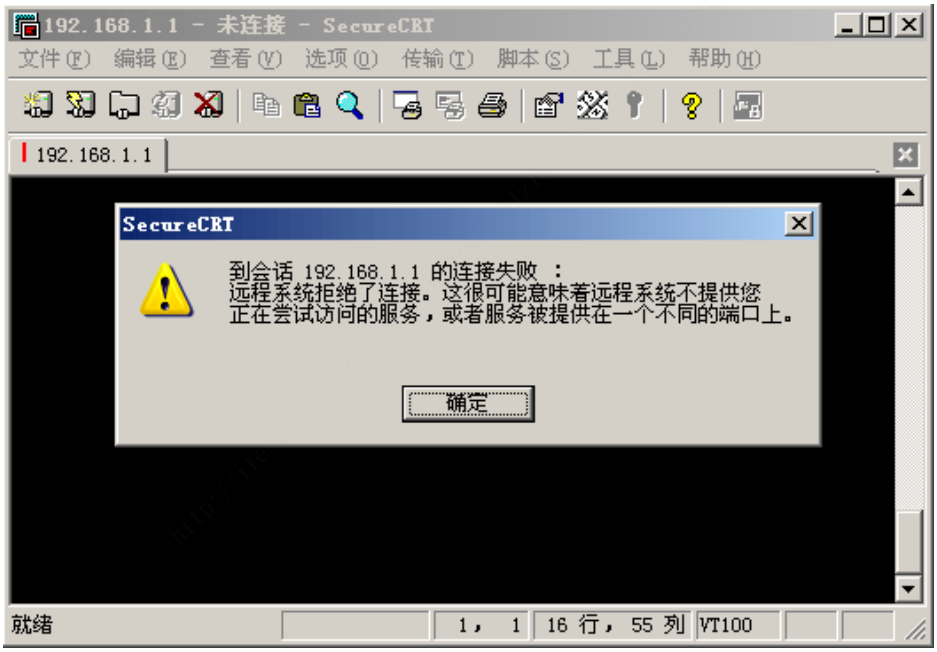
批注 [stanley888]：配置 SSH 的客户端的空闲超时时间为 30 秒。

批注 [stanley889]：配置 SSH 的客户端的失败次数。如果尝试失败次数超过指定端。则默认停止响应 120 秒。下面一条命令配置停止响应时间。

批注 [stanley890]：配置 VTY 的线路，接受 SSH 的接入。

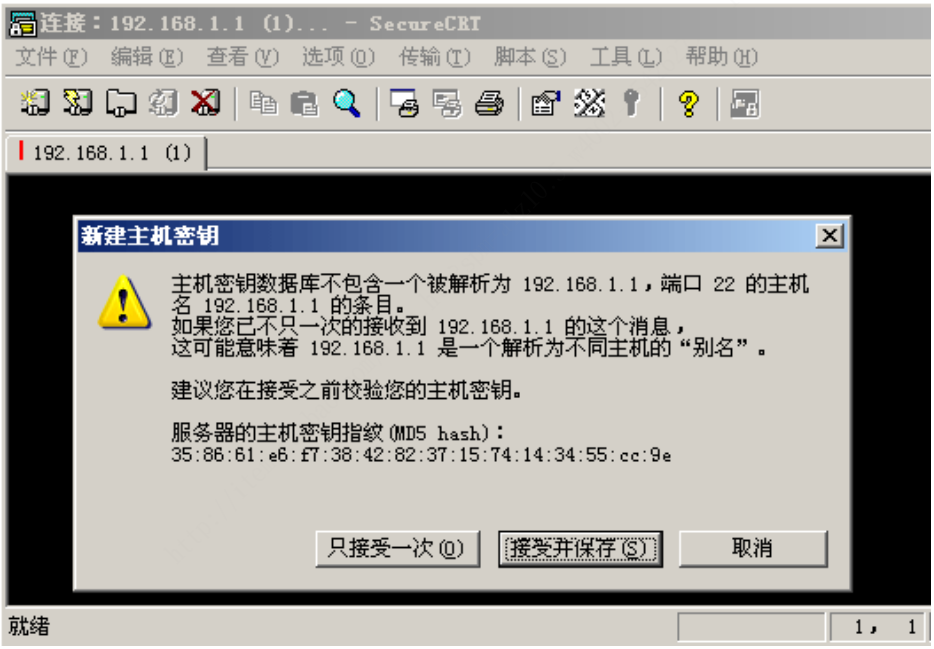
批注 [stanley891]：配置 SSH 的客户端的失败次数。如果尝试失败次数超过指定端。则默认停止响应 120 秒。下面一条命令配置停止响应时间。

7、完成 SSH 服务器端配置，在 PC 上再次使用 telnet 进行连接，显示连接出错：

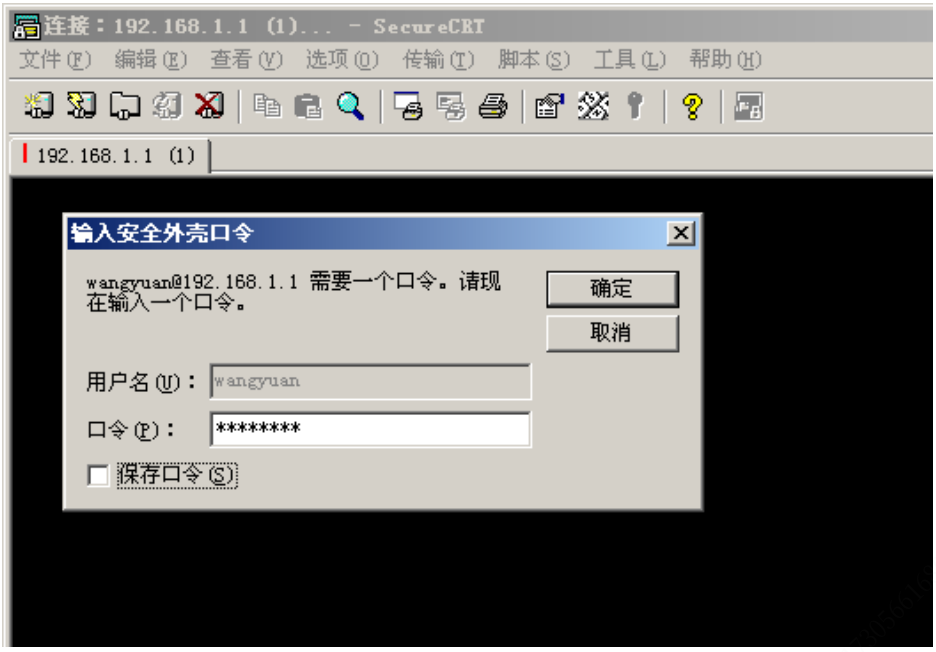


8、配置 SSH 的连接，同时还需要注意 Cisco 路由器不支持 SSH1 的 zlib 的压缩，而 secureCRT 默认是启了此压缩，因此需要编辑属性修改压缩属性：

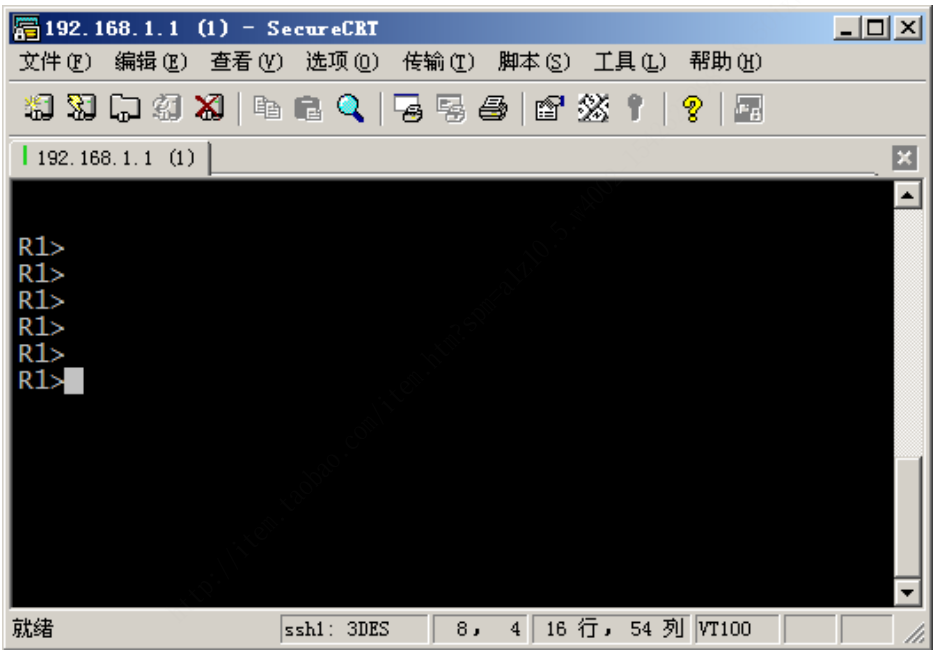
9、点击连接后，secureCRT 弹出如下窗口，要求接受服务器密钥，点击“接受并保存”或“只接受一次”的按钮继续：



10、接受密钥后，本地 secureCRT 会弹出要求提供密码的对话框：



11、在输入正确的密码后，即可以直接登录到 R1 路由器了，如下图所示：



12、当客户端登录成功后，在 R1 路由器上查看 SSH 的客户端连接：

```
R1#show ssh
Connection      Version   Encryption    State                Username
0               2         RSA           Session Started      wangyuan
```

12、实验完成。

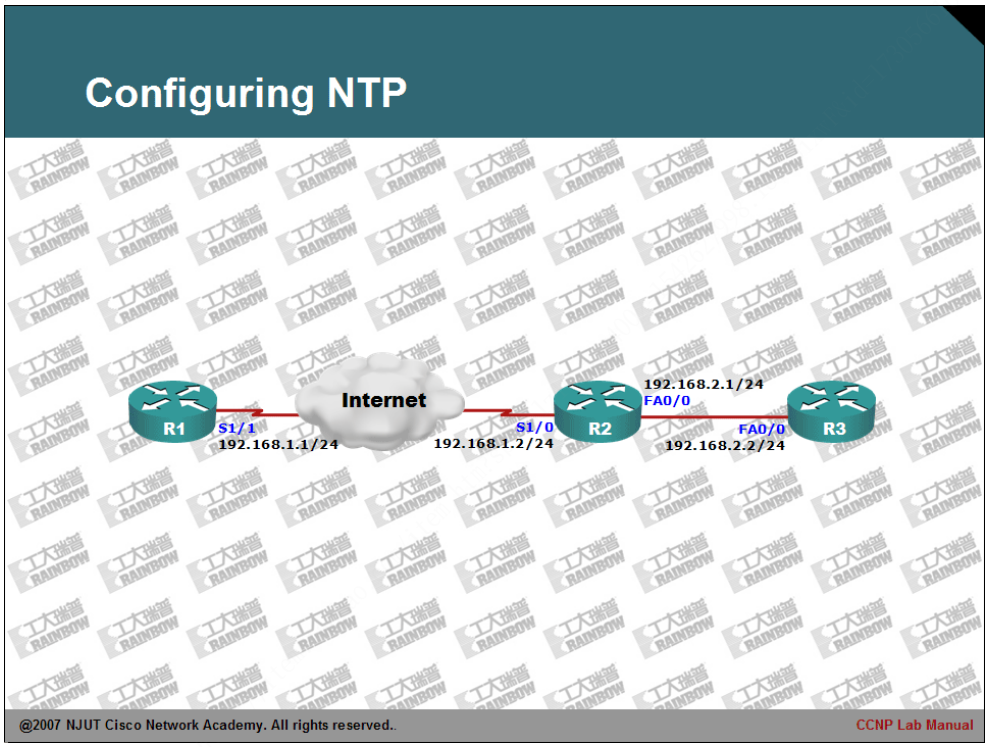
CCNP Lab Manual

Lab 74. Configuring NTP

实验目的：

1、掌握配置路由器交换机的时间及时区命令。
2、掌握 NTP 的配置过程。
3、监控时间服务。
4、配置 NTP 的安全。

实验拓扑图：



实验步骤及要求：

1、配置各台路由器的 IP 地址，并且使用 ping 命令确认各路由器的直连口的互通性。

2、为了能够观察实验结果，在 R2 与 R3 路由器，配置不同的时间，以示区别。

配置如下：

```
R2(config)#
R2(config)#clock timezone CHINA +8
R2(config)#exit
R2#clock set 1:00:00 1 sep 2007
R2#
```

批注 [stanley892]：配置路由器的时区信息。

批注 [stanley893]：配置 R2 路由器的时间为:2007 年 9 月 1 日,1 点整。

```
R3(config)#
R3(config)#clock timezone CHINA +8
R3(config)#exit
R3#clock set 2:00:00 2 sep 2007
R3#
```

批注 [stanley894]：需要同步的设备其时区配置必须与 NTP 服务器一致,否则可能会导致同步失败。

3、在 R1 上配置正确的时间，配置如下：

```
R1(config)#
R1(config)#clock timezone CHINA +8
R1(config)#exit
R1#clock set 11:45:00 11 sep 2007
R1#
```

4、查看三台路由器的时间：

```
R1#show clock  detail
11:46:06.259 CHINA Tue Sep 11 2007
Time source is user configuration
```

```
R2#show clock  detail
01:04:47.727 CHINA Sat Sep 1 2007
Time source is user configuration
R2#
```

批注 [stanley895]：此时，显示本地时间配置仍然来源于用户配置。

```
R3#show clock detail
02:02:52.331 CHINA Sun Sep 2 2007
Time source is user configuration
R3#
```

5、配置 R1 路由器 NTP 时间服务器，配置如下：

```
R1(config)#
```

```
R1(config)#ntp authenticate
R1(config)#
R1(config)#ntp master
R1(config)#
R1(config)#ntp authentication-key 1 md5 cisco@server@key
R1(config)#
R1(config)#ntp peer 192.168.1.2 key 1
R1(config)#
R1(config)#ntp source serial 1/1
R1(config)#
```

批注 [stanley896]：启用 NTP 的认证。

批注 [stanley897]：配置 R1 为一台权威的 NTP 服务器。

批注 [stanley898]：配置 NTP 的安全认证密码。

批注 [stanley899]：配置时间对等体设备，并且指出使用序号为 1 的密码配置。

批注 [stanley900]：配置 NTP 与其它 NTP 设备通信的源 IP 地址。

NTP 服务器分层提供服务，因此通过 ntp master 命令还可以指定时间服务器的层次，如果在网络中还有其它的主 NTP 服务器的话，则使用此条命令时要异常小心。

时间按 NTP 服务器的等级传播。按照离外部 UTC 源的远近将所有服务器归入不同的 Stratum（层）中。Stratum-1 在顶层，有外部 UTC 接入，而 Stratum-2 则从 Stratum-1 获取时间，Stratum-3 从 Stratum-2 获取时间，以此类推，但 Stratum 层的总数限制在 15 以内。所有这些服务器在逻辑上形阶梯式的架构相互连接，而 Stratum-1 的时间服务器是整个系统的基础。

在 Cisco 设备上层次的级别可能会影响路由器的时钟信息源。层次为 0 时，表明未指定层次级别或难以获得主要的参考时间源。层次为 1 时，表明使用了原子或无线电钟。思科不支持层次 1 的时钟服务。层次为 2-15 时，表时使用基于 GPS 的设备。思科支持此类设备，其可以连接到路由器上。层次为 16-255 时为保留选项。层使用 8bit 存储。默认情况下，在 CISCO 的设备上，层为 8。

6、配置 R2 路由器为 NTP 的中继路由器，其通过 R1 路由器，获得时间配置，然后将其广播给内部的其它路由器。配置如下：

```
R2(config)#ntp authenticate
R2(config)#
R2(config)#ntp authentication-key 1 md5 cisco@server@key
R2(config)#
R2(config)#ntp trusted-key 1
R2(config)#
R2(config)#ntp server 192.168.1.1
R2(config)#
R2(config)#ntp source fastEthernet 0/0
R2(config)#
R2(config)#ntp authentication-key 2 md5 cisco@client@key
```

批注 [stanley901]：打开 NTP 认证。

批注 [stanley902]：配置与 NTP 服务器认证的密码。

批注 [stanley903]：配置受信任的密钥定义。

批注 [stanley904]：配置 NTP 服务器的 IP。

批注 [stanley905]：配置如果自身向外广播时间时的源地址。

批注 [stanley906]：配置与 NTP 客户端认证的密码。

```
R2(config)#
R2(config)#interface fastEthernet 0/0
R2(config-if)#ntp broadcast key 2
R2(config-if)#exit
R2(config)#
```

批注 [stanley907]：配置 FA0/0 接口，进行 NTP 的广播。并且使用 key 2 密钥配置进行认证。

7、继续配置 R3 路由器为 NTP 的客户端。配置如下：

```
R3(config)#ntp authenticate
R3(config)#
R3(config)#ntp authentication-key 1 md5 cisco@client@key
R3(config)#
R3(config)#ntp trusted-key 1
R3(config)#
R3(config)#interface fastEthernet 0/0
R3(config-if)#ntp broadcast client
R3(config-if)#exit
R3(config)#exit
R3#
```

批注 [stanley908]：配置本地路由器为 NTP 的客户端。其会接收 NTP 的时间广播信息来配置本地时间。

8、稍等一段时间，等待时间同步后，查看 R1、R2 与 R3 的时间信息，确认已同步：

```
R1#show clock detail
12:31:20.135 CHINA Tue Sep 11 2007
Time source is NTP
```

```
R2#show clock detail
12:31:29.061 CHINA Tue Sep 11 2007
Time source is NTP
```

批注 [stanley909]：此时，已经显示时间源为 NTP 的服务器。

```
R2#show clock detail
12:45:48.913 CHINA Tue Sep 11 2007
Time source is NTP
```

9、在 R2 上查看 NTP 的关联状态：

```
R2#show ntp associations

      address         ref clock      st   when   poll reach   delay   offset    disp
*~192.168.1.1      127.127.7.1       8     59     64   377     3.9     0.18    18.3
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
R2#
```

10、查看 R2 的 NTP 的状态信息：

```
R2#show ntp status
Clock is synchronized, stratum 9, reference is 192.168.1.1
```

```
nominal freq is 250.0000 Hz, actual freq is 250.0012 Hz, precision is 2**18
reference time is CA909DAD.8651D35E (12:53:01.524 CHINA Tue Sep 11 2007)
clock offset is 0.1824 msec, root delay is 3.89 msec
root dispersion is 19.70 msec, peer dispersion is 19.50 msec
R2#
```

11、另外还可以使用如下命令调试 NTP：

```
R2#debug ntp authentication
R2#debug ntp packets
```

12、为了确保 NTP 的安全性，因此还建议在 R2 上配置如下 ACL 保护 NTP 的连接：

```
R2(config)#access-list 60 permit host 192.168.1.1
R2(config)#ntp access-group peer 60
```

13、对于 R3 的客户端，建议在其它的接口上关闭 NTP 的服务，示例如下：

```
R3(config)#interface fastEthernet 2/0
R3(config-if)#ntp disable
R3(config-if)#exit
```

批注 [stanley910]：配置此接口的 NTP 为禁用状态。

14、实验完成。

CCNP Lab Manual

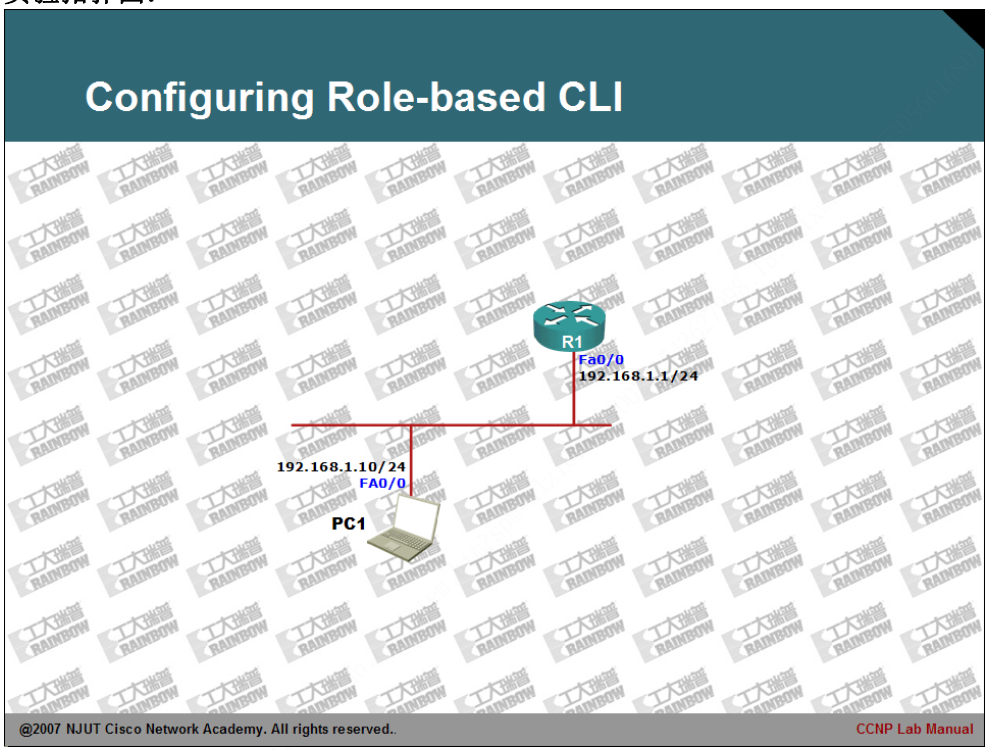
Lab 75. Configuring Role-Based CLI

实验目的：

1、掌握基于角色视图的命令行的权限配置。

2、确认角色视图的配置。

实验拓扑图：



实验步骤及要求：

1、配置路由器的 IP 地址，并且使用 Ping 命令确认路由器与 PC 机的直连口的互通。

2、为了能够在路由器上启用视图，需要启用 AAA，并且配置特权密码，用于根视图的登录。配置如下：

```
R1(config)#
R1(config)#aaa new-model
R1(config)#
R1(config)#enable secret cisco
R1(config)#
```

3、在 R1 路由器上，启用根视图，配置如下：

```
R1#
R1#enable view
Password: ******
R1#
*Sep 11 18:40:36.431: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1#
R1#
```

批注 [stanley911]：启用根视图。

批注 [stanley912]：根据系统提示，可以判断出目前已经进入到根视图模式。

4、在根视图模式下，为不同的管理需求配置不同的视图，配置如下：

```
R1(config)#
R1(config)#parser view monitor_view
R1(config-view)#
*Sep 11 18:43:22.395: %PARSER-6-VIEW_CREATED: view 'monitor_view' successfully created.
R1(config-view)#
R1(config-view)#secret cisco
R1(config-view)#
R1(config-view)#commands exec include show version
R1(config-view)#commands exec include all show ip
R1(config-view)#exit
R1(config)#
```

批注 [stanley913]：创建用于监测的视图。

批注 [stanley914]：为监测的视图配置密码。

批注 [stanley915]：配置此模式可以使用的命令列表。

5、继续在根视图模式下，配置用于调试的管理视图，配置如下：

```
R1(config)#
R1(config)#parser view debug_view
R1(config-view)#
*Sep 11 18:47:42.599: %PARSER-6-VIEW_CREATED: view 'debug_view' successfully created.
R1(config-view)#
R1(config-view)#secret cisco
R1(config-view)#
R1(config-view)#commands exec include debug ip ospf adj
```

批注 [stanley916]：创建用于调试的视图。

```
R1(config-view)#commands exec include debug ip rip
R1(config-view)#commands exec include debug ip bgp
R1(config-view)#commands exec include undebug all
R1(config-view)#
R1(config-view)#exit
R1(config)#
```

批注 [stanley917]: 配置此视图可使用的命令列表。

6、继续配置一个用于路由配置的管理视图，配置如下：

```
R1(config)#parser view config_view
R1(config-view)#
*Sep 11 18:50:40.591: %PARSER-6-VIEW_CREATED: view 'config_view' successfully created.
R1(config-view)#
R1(config-view)#secret cisco
R1(config-view)#
R1(config-view)#commands exec include configure terminal
R1(config-view)#commands configure include router
R1(config-view)#commands router include network
R1(config-view)#commands configure include no router
R1(config-view)#command router include no network
R1(config-view)#commands exec include show running-config
R1(config-view)#exit
R1(config)#
```

7、返回到特权模式，查看配置确认配置：

```
R1#
R1#show running-config
Building configuration...

.....


parser view monitor_view
 secret 5 $1$AdI5$/ukL4mmy3FtflMX9F/xGN1
 commands exec include all show ip
 commands exec include show version
 commands exec include show
!
parser view debug_view
 secret 5 $1$f6vv$BZSgSvaswhuj9j7QJl/gW1
 commands exec include undebug ip rip
 commands exec include undebug ip ospf adj
 commands exec include undebug ip ospf
 commands exec include undebug ip bgp
 commands exec include undebug ip
 commands exec include undebug all
```

```
 commands exec include undebug
 commands exec include debug ip rip
 commands exec include debug ip ospf adj
 commands exec include debug ip ospf
 commands exec include debug ip bgp
 commands exec include debug ip
 commands exec include debug all
 commands exec include debug
!
parser view config_view
 secret 5 $1$Qt7f$P9b0g8kgaL.TlijTvBhcd1
 commands router include network
 commands router include no network
 commands router include no
 commands configure include router
 commands configure include no router
 commands configure include no
 commands exec include configure terminal
 commands exec include configure
 commands exec include show running-config
 commands exec include show
!
end

R1#
```

8、查看当前视图模式：

```
R1#show privilege
Currently in View Context with view 'root'
R1#
```

批注 [stanley918]：显示出当前处于 root 视图模式。

9、注销当前会话，使用视图模式登录路由器，过程如下：

```
R1>
R1>enable view monitor_view
Password:

R1#
*Sep 11 18:57:46.183: %PARSER-6-VIEW_SWITCH: successfully set to view 'monitor_view'.
R1#
R1#show privilege
Currently in View Context with view 'monitor_view'
R1#
R1#show ?
  bootflash:  display information about bootflash: file system
```

批注 [stanley919]：显示出当前处于monitor_view视图模式。

批注 [stanley920]：使用?号确认当前可以使用的命令。

```
  disk0:      display information about disk0: file system
  disk1:      display information about disk1: file system
  flash:      display information about flash: file system
  ip          IP information
  slot0:      display information about slot0: file system
  slot1:      display information about slot1: file system
  version     System hardware and software status

R1#show ip ?
  accounting              The active IP accounting database
  admission               Network Admission Control information
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  auth-proxy              Authentication Proxy information
.....
```

批注 [stanley921]：使用 show ip ?查看可以查看的子参数。

10、注销之前的会话，使用 debug 视图登录，进行确认：

```
R1>
R1>enable view debug_view
Password:

R1#
*Sep 11 19:00:38.995: %PARSER-6-VIEW_SWITCH: successfully set to view 'debug_view'.
R1#
R1#show privilege
Currently in View Context with view 'debug_view'
R1#
R1#show ?
% Unrecognized command
R1#
R1#debug ip ?
  bgp   BGP information
  ospf  OSPF information
  rip   RIP protocol transactions

R1#debug ip ospf ?
  adj  OSPF adjacency events

R1#
```

批注 [stanley922]：显示出当前处于 debug_view 视图模式。

批注 [stanley923]：由于没有授权，因此无法执行 show 命令。

批注 [stanley924]：使用 debug ip ?命令，可以看出其列出的项目，均为配置指定的项目。

批注 [stanley925]：对于 ospf 来说，也只有 adj 关系可以调试。

11、注销之前的会话，使用 config 视图进行登录，过程如下：

```
R1>
R1>enable view config_view
```

```
Password:

R1#
*Sep 11 19:03:58.947: %PARSER-6-VIEW_SWITCH: successfully set to view 'config_view'.
R1#
R1#show privilege
Currently in View Context with view 'config_view'
R1#
R1#show ?
  bootflash:      display information about bootflash: file system
  disk0:          display information about disk0: file system
  disk1:          display information about disk1: file system
  flash:          display information about flash: file system
  running-config  Current operating configuration
  slot0:          display information about slot0: file system
  slot1:          display information about slot1: file system
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#router rip
R1(config-router)#network 10.0.0.0
R1(config-router)#end
*Sep 11 19:05:31.619: %SYS-5-CONFIG_I: Configured from console by consolerouter
R1#
R1#show running-config
Building configuration...

Current configuration : 48 bytes
!
router rip
 network 10.0.0.0
!
!
end

R1#
```

批注 [stanley926]: 显示出当前处于 config_view 视图模式。

批注 [stanley927]: 只有被授权的命令，方可以执行。

批注 [stanley928]: 成功的进入到配置模式。

批注 [stanley929]: 可以进行 RIP 的配置。

批注 [stanley930]: 可以配置路由的网络。

批注 [stanley931]: 查看配置。

批注 [stanley932]: 只有被授权的配置项目，才可以被查看其配置。

12、通过以上配置，可以看出通过 view 模式配置路由器的权限，非常灵活多变。可以满足各种配置的需求。

13、实验完成。

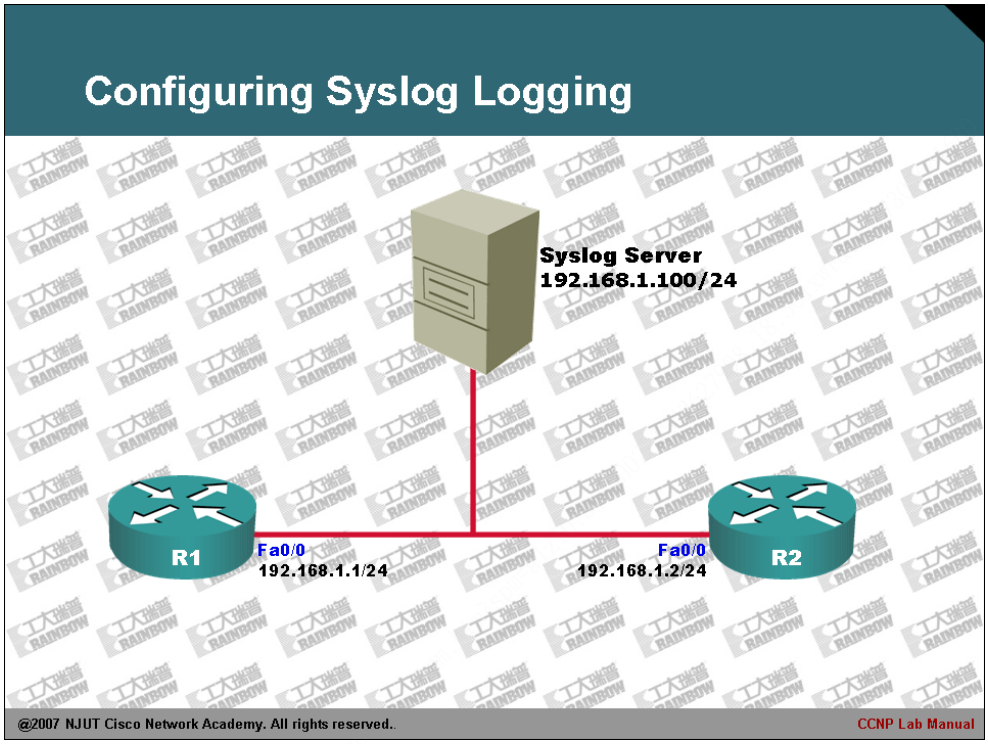
CCNP Lab Manual

Lab 76. Configuring Syslog Logging

实验目的：

1、掌握如何在路由器上配置 syslog 客户端。

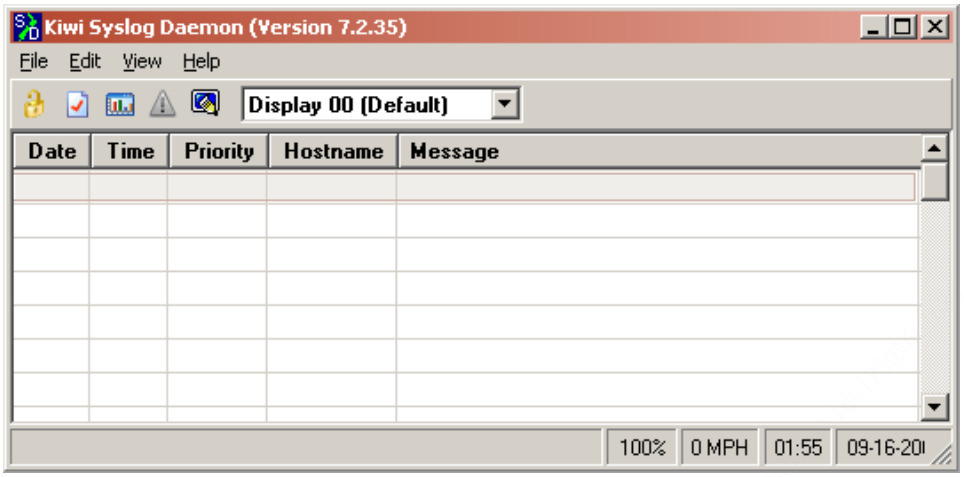
实验拓扑图：



实验步骤及要求：

1、根据拓扑，配置 R1，R2 路由器和 PC 主机的 IP 地址，并且使用 ping 命令确认连接。

2、在 PC 主机上安装 Syslog 服务器端软件，同时启动 Syslog 软件。本实验采用的免费的 Kiwi Syslog 的 Ver 7.2.35 版本日志服务器软件。如下图所示：



3、配置 R1 路由器为 Syslog 客户端，配置如下：

```
R1(config)#
R1(config)#logging 192.168.1.100
R1(config)#
R1(config)#logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>


R1(config)#logging trap
R1(config)#
R1(config)#logging source-interface fastEthernet 0/0
R1(config)#
R1(config)#logging facility ?
```

批注 [stanley933]：配置日志服务器的 IP 地址。

批注 [stanley934]：使用?号可以查看需要发送的日志类型。

批注 [stanley935]：本实验默认发送所有日志消息。如果在非实验环境，请注意本命令会对路由器产生较大负载，谨慎使用本命令。

批注 [stanley936]：配置日志服务器的记录源地址。

批注 [stanley937]：配置消息设备的类型。

```
  auth     Authorization system
  cron     Cron/at facility
  daemon   System daemons
  kern     Kernel
  local0   Local use
  local1   Local use
  local2   Local use
  local3   Local use
  local4   Local use
  local5   Local use
  local6   Local use
  local7   Local use
  lpr      Line printer system
  mail     Mail system
  news     USENET news
  sys10    System use
  sys11    System use
  sys12    System use
  sys13    System use
  sys14    System use
  sys9     System use
  syslog   Syslog itself
  user     User process
  uucp     Unix-to-Unix copy system

R1(config)#logging facility local7
R1(config)#
R1(config)#logging on
```

批注 [stanley938]: Cisco 路由器默认采用 local7 的类型发送消息。

批注 [stanley939]: 启用日志服务客户端功能。

关于设备类型的一些解释列表：

Auth 认证系统	**Cron** 时钟守护进程设备	**Daemoon** 系统守护进程	**Kern** 内核
Local 0 - 7 本地定义的消息	**Lpr** 打印机系统	**Mail** 邮件系统	**News** USENET 新闻
Sys 9 - 14 系统使用	**Syslog** 系统日志	**User** 用户进程	**Uucp** Unix 到 Unix 系统复制

4、为了能够触发日志消息的发送，在 R1 路由器上从全局配置模式使用 exit 命令退出到特权模式，以便于产生日志。观察路由器的提示：

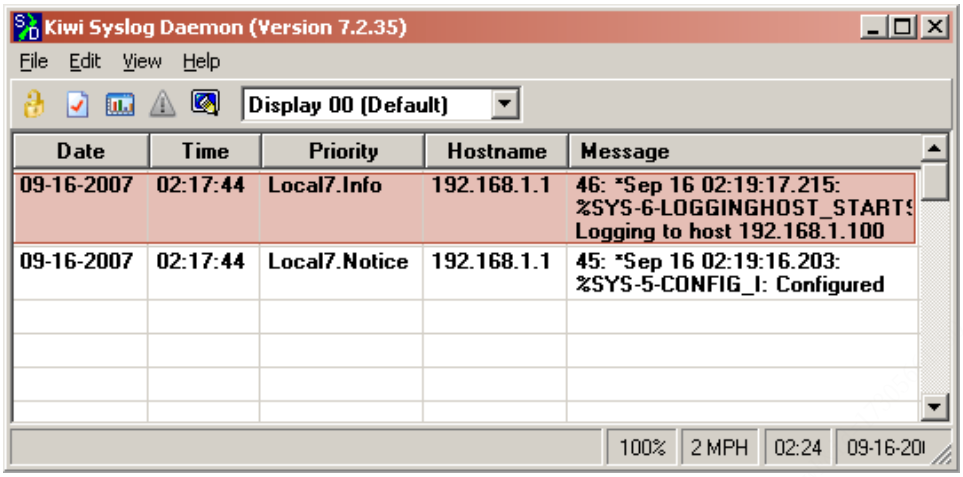
```
R1(config)#exit
R1#
*Sep 16 02:19:16.203: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

批注 [stanley940]: 退出全局配置模式的 SYS_5 级别的日志。即 Notifications（正常但重要的情况）日志。

```
*Sep 16 02:19:17.215: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.100 Port 514
started - CLI initiated
R1#
R1#
```

批注 [stanley941]：随后显示的消息，指出日志服务已经开始初始化。

5、查看 Syslog 服务器端的窗口消息显示，如下图所示：



5、配置两台路由器的 OSPF 路由协议，确认 Syslog 服务器是否可以捕获消息级别为 4 的 LOG_WARNING 警告消息，在配置过程中，请故意将两台 OSPF 路由器的 RouterID 配置相同，以便产生系统的 Debug 消息。配置如下所示：

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#router-id 1.1.1.1
R1(config-router)#exit
```

批注 [stanley942]：指定 R1 的 RouterID 为 1.1.1.1。

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#router-id 1.1.1.1

Reload or use "clear ip ospf process" command, for this to take effect
R2(config-router)#end
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
R2#
```

批注 [stanley943]：配置与 R1 路由器相同的 RouterID。

批注 [stanley944]：系统提示需要使用 clear ip ospf process 命令，重启 OSPF 进程。

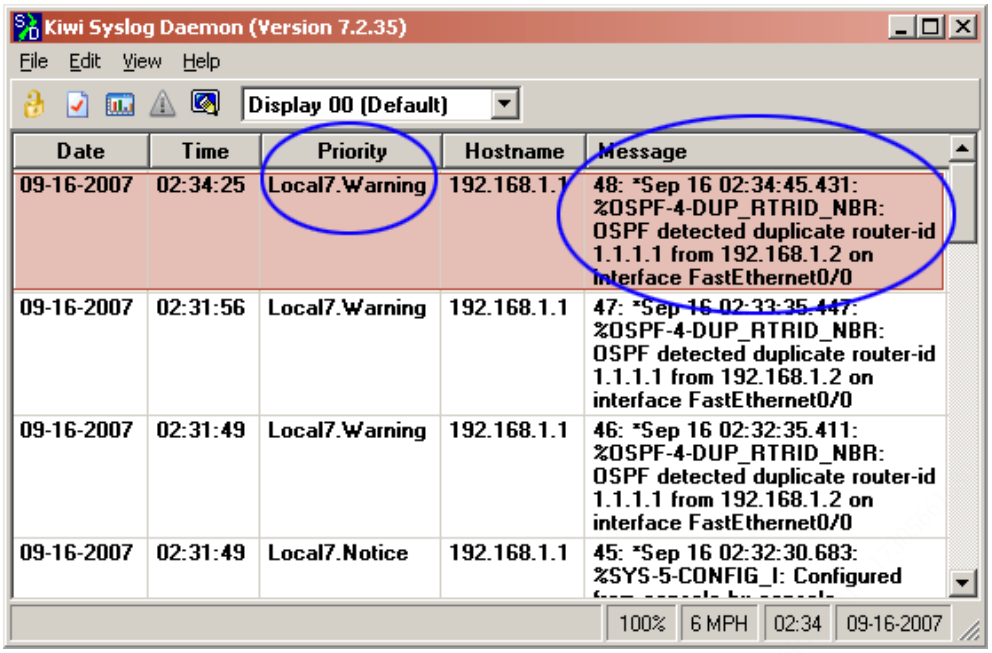
6、观察 R1 路由器系统提示：

```
R1#
*Sep 16 02:32:35.411: %OSPF-4-DUP_RTRID_NBR: OSPF detected duplicate router-id 1.1.1.1 from
192.168.1.2 on interface FastEthernet0/0
```

批注 [stanley945]：系统提示 OSPF 的 RouterID 重复。

```
R1#
```

7、查看 Syslog 窗口，观察信息。如下图所示：



8、从以上截图可以看出Syslog成功的记录了客户端的OSPF路由协议的RouterID重复问题。

9、**再次提示：**在真实的网络环境中如果直接使用 loggin trap 命令，而不指定需要记录的日志消息级别，极有可能直接导致路由负载过重而当机。切记！

10、实验完成。