

1. CCNP BSCI 课程	6
1.1. EIGRP 增强型内部网关路由协议	6
1.1.1. EIGRP的特性:	6
1.1.2. EIGRP的关键技术	6
1.1.3. EIGRP的术语	6
1.1.4. EIGRP的包的类型	6
1.1.5. EIGRP metric值的计算	7
1.1.6. EIGRP的配置	7
1.1.7. 路由汇总	9
1.1.8. 非等价负载均衡	10
1.1.9. 基于MD5 的认证加密	10
1.2. OSPF 开放式最短路径优先协议	11
1.2.1. 工作的过程	11
1.2.2. OSPF的区域划分	11
1.2.3. 关于OSPF的邻居关系与邻接关系	12
1.2.4. OSPF包的类型	12
1.2.5. DR和BDR的选举	13
1.2.6. OSPF的实验配置	13
1.2.7. Router-id 的选举	14
1.2.8. OSPF网络类型	14
1.2.9. Virtual-Link 虚链路	16
1.2.10. LSA(链路状态通知) 的类型	17
1.2.11. 路由的类型	20
1.2.12. 修改OSPF接口COST值和路由器的带宽值	20
1.2.13. OSPF的特殊区域	20
1.2.14. OSPF的邻居认证	23
1.2.15. OSPF的路由汇总	24
1.3. IS-IS(中间系统) 路由协议	24
1.3.1. 基本概念	24
1.3.2. 相关术语	25
1.3.3. 相关特性	25
1.3.4. Level-1 和 Level-2 以及 Level-1-2	25
1.3.5. NSAP地址	25
1.3.6. IS-IS的邻居建立条件	26
1.3.7. 纯IS-IS的实验配置	26
1.3.8. 集成IS-IS的实验配置	28
1.4. BGP 边界网关协议	30
1.4.1. 何时使用BGP	30
1.4.2. 满足以下条件之一时, 不要使用BGP	30
1.4.3. BGP的特性	31
1.4.4. BGP的数据库	31
1.4.5. BGP的消息类型	31
1.4.6. 关于IBGP与EBGP之间的关系	31
1.4.7. 基本BGP邻居建立的实验	33
1.4.8. 高级的BGP(属性)实验	34
1.4.9. BGP的路径属性	37

1.4.10.	BGP路由选择决策过程	37
1.4.11.	使用Route-map操纵BGP路径实验(Local_prefence As-path)	38
1.5.	过滤路由的更新	40
1.6.	路由重分发(Redistribution)	41
1.6.1.	将RIPv2 路由重分发进 OSPF 中	41
1.6.2.	将OSPF路由重分发进RIPv2 中	41
1.6.3.	将EIGRP 100 重分发进OSPF 中	42
1.6.4.	将OSPF重分发进EIGRP 100 中	42
1.6.5.	将RIP v2 重分发进EIGRP 100 中	43
1.6.6.	将EIGRP 100 重分发进 RIPv2 中	43
1.6.7.	将EIGRP 100 重分发进 EIGRP 10	43
1.6.8.	将EIGRP 100 重分发进 集成ISIS中	44
1.6.9.	将ISIS 重分发进EIGRP 100	45
1.6.10.	将ISIS重发分进OSPF中	45
1.6.11.	将OSPF 重分发进ISIS中	46
1.7.	各种路由协议的管理距离值	46
1.8.	(MultiCast)组播	47
1.8.1.	单播数据流	47
1.8.2.	广播数据流	47
1.8.3.	组播数据流	48
1.8.4.	组播的缺点:	48
1.8.5.	IP的组播地址(3 层地址)	49
1.8.6.	数据链路层的 2 层组播地址	49
1.8.7.	IGMP互联网组管理协议	50
1.8.8.	第 2 层组播帧交换	51
1.8.9.	组播路由协议	51
1.8.10.	带有RP的稀疏密集的实验配置	52
1.9.	IPV6	52
1.9.1.	IPV6 的特性	52
1.9.2.	地址空间	53
1.9.3.	IPv6 的地址格式	53
1.9.4.	IPv6 地址类型	53
1.9.5.	组播地址 Multicast	54
1.9.6.	任意播地址 Anycast	55
1.9.7.	EUI(扩展全局标识)地址格式	55
1.9.8.	IPv6 与 OSPFv3 的实验配置	56
2.	CCNP BCMSN课程	57
2.1.	VLAN(虚拟局域网)	57
2.1.1.	概念:	57
2.1.2.	VLAN的创建	58
2.1.3.	VLAN的划分(将相应的接口划分到相应的VLAN)	58
2.1.4.	关于TRUNK链路 (中继链路)	58
2.1.5.	TRUNK链路的配置	58
2.1.6.	关于DTP协议 (动态中继协议)	59
2.1.7.	VTP 协议(VLAN中继协议)	59
2.1.8.	VTP的实验配置:	60

2.2.	Spanning tree protocol (STP)生成树协议	61
2.2.1.	冗余网络中产生的问题	61
2.2.2.	冗余网络的解决方法	61
2.2.3.	BPDU(桥协议数据单元)概念	61
2.2.4.	Bridge ID(网桥标识符)概念	61
2.2.5.	根桥的选举	62
2.2.6.	非根桥中根端口的选举和指定端口的选举	62
2.2.7.	生成树协议的端口状态	62
2.2.8.	常用增强型生成树协议:	62
2.2.9.	高级的STP特性	62
2.2.10.	提高生成树的弹性机制	63
2.2.11.	MSTP 多生成树协议	63
2.3.	2 层/3 层 VLAN间路由	64
2.3.1.	单臂路由(2 层交换机+ 路由器)实现VLAN间通信	64
2.3.2.	多层交换机实现VLAN间路由实验	65
2.4.	HSRP 热备份冗余路由协议	66
2.4.1.	HSRP的概念	66
2.4.2.	HSRP技术在网络中的应用	67
2.4.3.	HSRP的实验	67
2.5.	VRRP 虚拟路由器冗余协议	69
2.5.1.	VRRP 虚拟路由器冗余协议	69
2.6.	GLBP 网关负载均衡协议	70
2.6.1.	GLBP 网关负载均衡协议	70
2.7.	WLAN(无线局域网)	72
2.7.1.	WLAN的无线技术标准	72
2.7.2.	WLAN的基本概念	72
2.7.3.	SSID(服务集标识符)	72
2.7.4.	无线应用技术标准	72
2.7.5.	无线的安全	72
2.7.6.	使用WEB方式配置无线AP设备	73
2.8.	以太网通道(链路汇聚)	74
2.8.1.	特点:	74
2.8.2.	链路汇聚协议	74
2.8.3.	二层Etherchannel实验配置	74
2.8.4.	三层Etherchannel实验配置	75
2.9.	交换机的端口安全(Port Security)	76
2.9.1.	在交换机的接口下配置端口安全	76
2.9.2.	在交换机上实施IP与MAC的双向绑定	76
2.10.	pVLAN(私有VLAN)	77
2.10.1.	概念术语	77
2.10.2.	实验拓扑及配置	77
2.11.	DHCP Snooping/ IPSG /DAI	79
2.11.1.	关于DHCP的欺骗攻击	79
2.11.2.	解决DHCP的欺骗攻击(DHCP Snooping DHCP监听)	79
2.11.3.	DHCP Snooping实验配置步骤	79
2.11.4.	IPSG (IP的源防护)	80

2.12.	DAI(动态ARP检测)	81
2.12.1.	DAI(动态ARP检测)	81
2.12.2.	DAI的作用	81
2.12.3.	配置SW1 的防护功能	81
2.13.	创建多用户授权	83
2.13.1.	关于用户帐号的安全级别（1-15）	83
2.13.2.	创建用户	83
2.13.3.	给自定义用户授予命令权限	83
2.14.	AAA	84
2.14.1.	AAA	84
2.15.	SNMP简单网络管理协议	85
2.15.1.	SNMP简单网络管理协议	85
3.	CCNP ISCW课程	85
3.1.	DSL技术	85
3.1.1.	概念：	85
3.1.2.	DSL技术的比较	86
3.1.3.	DSL的数据传输距离的比较	86
3.1.4.	使用路由器做PPPoE的客户端连接	86
3.2.	MPLS(多协议标签交换)	88
3.2.1.	MPLS术语	88
3.2.2.	MPLS的架构	89
3.2.3.	PHP(倒数第二跳弹出)	89
3.2.4.	MPLS转发实验	90
3.3.	IPsec (IP的安全)	95
3.3.1.	IPsec的基概念	95
3.3.2.	IPsec的主要协议	95
3.3.3.	安全算法	96
3.3.4.	IKE的工作阶段	96
3.3.5.	关于ESP和AH	96
3.3.6.	关于隧道模式和传输模式	97
3.4.	站点VPN (Site to Site VPN)	99
3.4.1.	配置Cisco路由器支持SDM管理软件的连接	99
3.4.2.	SDM软件的安装及需要修改的文件信息	99
3.4.3.	使用SDM工具配置 Site to Site VPN	99
3.5.	GRE over IPsec 通用路由封装	105
3.5.1.	GRE的基本概念	105
3.5.2.	GRE链路的配置要求	105
3.5.3.	使用SDM配置GRE over IPsec实验	105
3.6.	Cisco Easy VPN	114
3.6.1.	组成部分	114
3.6.2.	前期配置步骤	114
3.7.	DMVPN动态多点VPN	122
3.7.1.	DMVPN的特性：	122
3.7.2.	实验拓扑图	122
3.8.	启用SSH进行远程登陆	133
3.8.1.	启用SSH进行远程登陆	133

4.	CCNP ONT 课程	134
4.1.	QOS(服务质量保证)	134
4.1.1.	QoS的概念:	134
4.1.2.	QoS的服务模型.....	134
4.1.3.	数据包(ToS)和数据帧(CoS)的分类	134
4.1.4.	拥塞管理(队列管理)	135
4.1.5.	拥塞避免(丢弃策略)	137
4.1.6.	实验安全配置	138
4.2.	CAR(承诺访问速率).....	141
4.2.1.	CAR(承诺访问速率).....	141
4.3.	拓扑图制作及综合实验	142
4.3.1.	配置步骤:	143
4.3.2.	整个实验的完整配置	143

1. CCNP BSCI 课程

1.1. EIGRP 增强型内部网关路由协议

1.1.1. EIGRP的特性:

- 属 CISCO 私有协议
- 高级的距离矢量路由协议
- 实现网络的快速收敛
- 支持变长子网掩码和不连续的子网
- 路由更新时发送变化部分的更新内容
- 路由更新采用触发更新机制，只当网络发生变化时，才会发送路由更新
- 支持多个网络层的协议(IP、IPX、Novell 协议)
- 使用组播和单播技术代替了广播(组播地址: 224.0.0.10)
- 在网络的任意点可方便的创建手动路由汇总
- 实现 100%无环路(基于 DUAL(弥散更新算法))
- 支持等价的和非等价的负载均衡

1.1.2. EIGRP的关键技术

- 邻居的发现和恢复使用 Hello 包来建立，高速链路 5 秒发送 Hello 包，低速链路是 60 秒发送 Hello 包
- 是一个 RTP(可靠的传输协议)协议，能够保证所有的更新数据包能被邻居路由器接受到
- 使用 DUAL 算法机制，选择一个低代价、无环路的路径到达每一个目标段

1.1.3. EIGRP的术语

- 1、Successor 后继路由 \ 主路由
- 2、Feasible Successor (FS)可行后继路由 \ 备用路由
- 3、Feasible Distance (FD)可行距离 \ 指从源到达目标段的路径距离值
- 4、Advertised Distance (AD)通告距离 \ 是指通告路由器到达目标段的距离值

1.1.4. EIGRP的包的类型

- Hello
- Update 更新包
- Query 查询包
- Reply 应答包
- ACK 确认包

Router# debug eigrp packet //关闭 debug 使用 undebug all

1.1.5. EIGRP metric值的计算

- K1= 带宽 1 BW
- K2= 负载 0 txload(发送) 1/255 rxload(接收) 1/255 255 代表固定参考值
- K3= 延迟 1 DLY 100M=100 10M=1000 1.544M=20000
- K4= 可靠性 0 Reliability 255/255 (最可靠)
- K5= 最大传输单元 0 MTU 1500

注：1 代表使用, 0 代表未被使用

Router# show interface E0/0

计算公式

$$\text{Metric} = [10^7 / \text{最小带宽}(k) + (\text{延迟}) / 10] \times 256$$

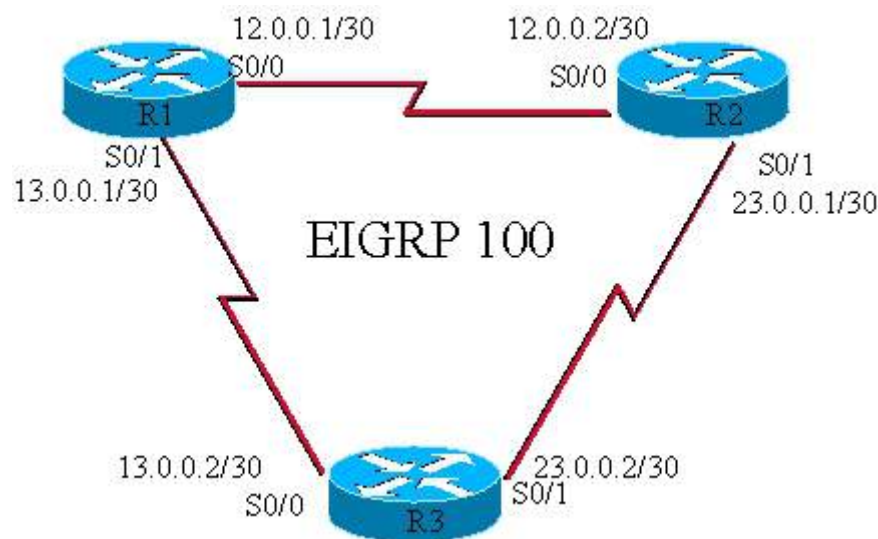
说明： 最小带宽：指从源到达目的网段链路中的最小带宽

延迟： 指每段链路的延迟总和

1.1.6. EIGRP的配置

实验目的：各路由器之间使用 EIGRP 路由协议实现互连互通

实验拓扑图如下：



各路由器的实验配置如下：

```
R1(config)# router eigrp 100
```

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

```
R1(config-router)# network 12.0.0.0 0.0.0.3
```

```
R1(config-router)# network 13.0.0.0 0.0.0.3
```

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

```
R2(config)# router eigrp 100
```

```
R2(config-router)# no auto-summary
```

```
R2(config-router)# network 12.0.0.0 0.0.0.3
```

```
R2(config-router)# network 23.0.0.0 0.0.0.3
```

```
R2(config-router)# end
```

```
R3(config)# router eigrp 100
R3(config-router)# no auto-summary
R3(config-router)# network 13.0.0.0 0.0.0.3
R3(config-router)# network 23.0.0.0 0.0.0.3
R3(config-router)# end
```

```
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

```
23.0.0.0/30 is subnetted, 1 subnets
D      23.0.0.0 [90/2681856] via 13.0.0.2, 00:00:12, Serial0/1
        [90/2681856] via 12.0.0.2, 00:00:12, Serial0/0
12.0.0.0/30 is subnetted, 1 subnets
C      12.0.0.0 is directly connected, Serial0/0
13.0.0.0/30 is subnetted, 1 subnets
C      13.0.0.0 is directly connected, Serial0/1
```

说明: [90/2681856] [协议管理距离/Metric 度量值]

```
R1#show interfaces s0/0
```

Serial0/0 is up, line protocol is up

Hardware is M4T

Internet address is 12.0.0.1/30

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255

Metric= [107/最小带宽(k) + (延迟+延迟)/10] × 256

Metric= [107/1544 + 4000] × 256

Metric= [6476 + 4000] × 256

Metric= 2681856

说明: 当 107/1544 时候, 会出现小数点, 立即取整数位, 舍弃小数点。

```
R1# show ip eigrp topology
```

```
P 23.0.0.0/30, 2 successors, FD is 2681856
    via 13.0.0.2 (2681856/2169856), Serial0/1
    via 12.0.0.2 (2681856/2169856), Serial0/0
```

```
R1# config ter
```

```
R1(config)# interface s0/0
```

```
R1(config-if)# bandwidth 1540
```

```
R1(config-if)# end
```

```
R1# show ip eigrp topology
```


P 23.0.0.0/30, 1 successors, FD is 2681856
 via 13.0.0.2 (2681856/2169856), Serial0/1
 via 12.0.0.2 (2686208/2169856), Serial0/0

结论：路由中的 Metric= Successor 值= 最小的 FD 值

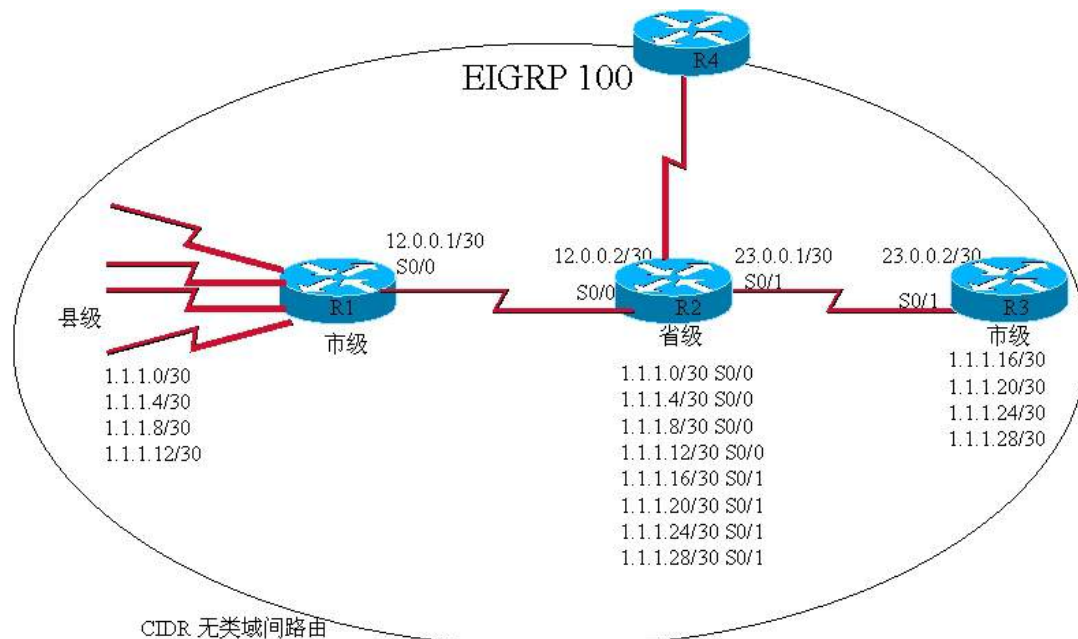
R1#show ip eigrp neighbors //查看邻居信息

1.1.7. 路由汇总

实验目的：将市级网络的路由发往省级设备时做手动路由汇总

默认情况下，EIGRP 是自动开启路由汇总功能的(Auto-Summary)

实验拓扑图如下所示：



1.1.1.0/30	11111111.11111111.11111111.00000000	1.1.1.16/30	11111111.11111111.11111111.00010000
1.1.1.4/30	11111111.11111111.11111111.00000100	1.1.1.20/30	11111111.11111111.11111111.00010100
1.1.1.8/30	11111111.11111111.11111111.00001000	1.1.1.24/30	11111111.11111111.11111111.00011000
1.1.1.12/30	11111111.11111111.11111111.00001100	1.1.1.28/30	11111111.11111111.11111111.00011100
1.1.1.0/28		1.1.1.16/28	

R1(config)# interface S0/0

R1(config-if)# ip summary-address eigrp 100 1.1.1.0 255.255.255.240

R1(config-if)# end

R3(config)# interface S0/1

R3(config-if)# ip summary-address eigrp 100 1.1.1.16 255.255.255.240

R3(config-if)# end

R2#show ip route

D 1.1.1.0 [90/2297856] via 12.0.0.1, 00:03:18, Serial0/0

D 1.1.1.16 [90/2297856] via 23.0.0.2, 00:00:02, Serial0/1

1.1.8. 非等价负载均衡

计算公式：

$\text{Variance 值} \times (\text{Successor})\text{FD 值} \geq (\text{FS})\text{FD 值}$

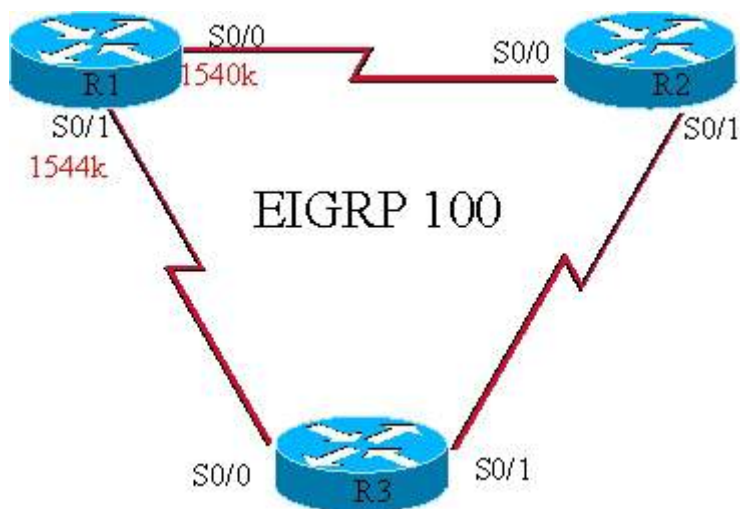
符合公式，即非等价负载均衡的条件成立

实验目的：在 R1 上实现非等价负载均衡

实验拓扑图如下：

将 R1 路由器的 S0/0 接口带宽修改为：1540K

R1(config-if)#bandwidth 1540 //修改接口参考带宽命令



实验配置和输出结果如下：

R1# show ip eigrp topology

P 23.0.0.0/30, 1 successors, FD is 2681856

via 13.0.0.2 (2681856/2169856), Serial0/1

via 12.0.0.2 (2686208/2169856), Serial0/0

R1# config t

R1(config)#router eigrp 100

R1(config-router)# variance 2 //设置非等价负载均衡的 variance 倍数为 2

R1(config-router)#end

R1#show ip route

D 23.0.0.0 [90/2681856] via 13.0.0.2, 00:00:10, Serial0/1

[90/2686208] via 12.0.0.2, 00:00:10, Serial0/0

上述非等价负载均衡条件成立

1.1.9. 基于MD5 的认证加密

实验目的：在 R1 和 R2 的链路之间启用基于 MD5 的邻居认证加密

详细配置如下：

R1(config)# interface S0/0

R1(config-if)# ip authentication mode eigrp 100 md5 //在接口下启用认证

```

R1(config-if)# ip authentication key-chain eigrp 100 TEST-KEY
R1(config-if)# exit
R1(config)# key chain TEST-KEY
R1(config-key-chain)# key 99      //邻居间的 key id 必须一致
R1(config-keychain-key)#key-string cisco
R1(config-keychain-key)#end

R2(config)# interface S0/0
R2(config-if)# ip authentication mode eigrp 100 md5    //在接口下启用认证
R2(config-if)# ip authentication key-chain eigrp 100 TEST-KEY //名称只是本地有效
R2(config-if)# exit
R2(config)# key chain TEST-KEY
R2(config-key-chain)# key 99      //邻居间的 key id 必须一致
R2(config-keychain-key)#key-string cisco
R2(config-keychain-key)#end

```

1.2. OSPF 开放式最短路径优先协议

1.2.1. 工作的过程

- 邻居表的形成：在运行 OSPF 的路由器之间，发送 Hello 包（每隔 10 秒发送一次或每隔 30 秒发送一次）

Router# show ip ospf neighbors //查看邻居表

- 拓扑表的形成：

- ✧ 在所有形成邻接关系的路由器之间分发 LSA(链路状态通告)
- ✧ 在收到由邻居路由器发送来的 LSA 后，会把它加入到自己的 LSDB(链路状态数据库)中，然后发送一份完整的拷贝给该路由器的其它邻居
- ✧ 最终，LSA 会在整个区域中泛洪，所有的路由器都会形成同样的 LSDB
- ✧ 每台路由器都会以自己为根，使用 SPF 算法，构建出一个前往目的地得最佳且最短的路径

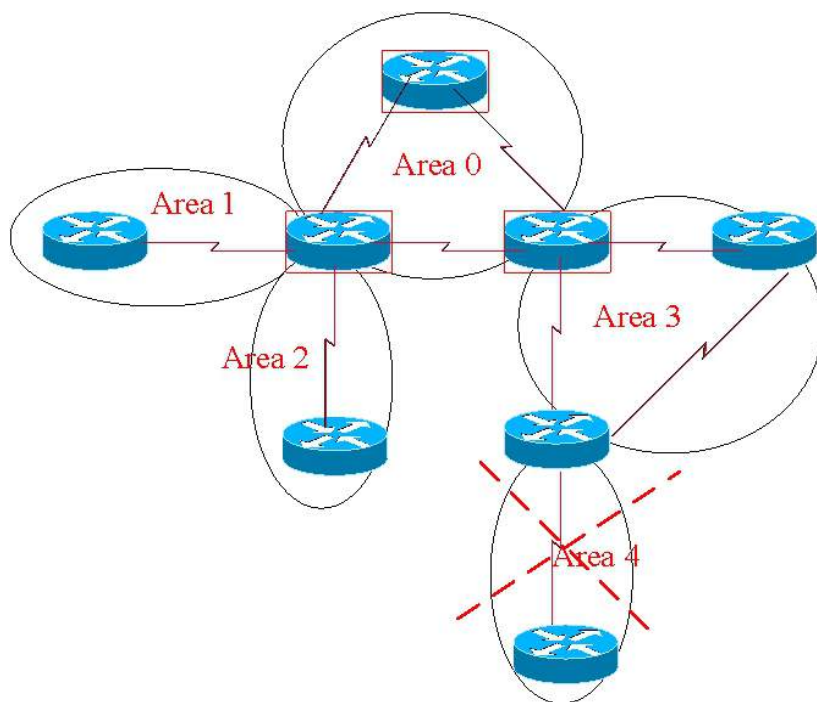
Router# show ip ospf database //查看 OSPF 的拓扑表

- 路由表的形成：路由表中存储的是 OSPF 的最佳且可达的无环路的路由信息

1.2.2. OSPF的区域划分

- 主干区域 Area 0
- 常规区域 除 Area0 之外的所有其它区域

说明：OSPF 要求，所有的常规区域，必须和主干区域相连



ABR: 区域边界路由器

ASBR: 连接外部自治系统的区域边界路由器

1.2.3. 关于OSPF的邻居关系与邻接关系

- OSPF 的邻居关系(Neighbor): 能够互相发送或接收 HELLO 包, 双向交互 Router-id 信息 (双向认识的过程)

说明: 建立邻居的要求:

- ✧ Hello 包的发送时间间隔和死亡间隔需一致
- ✧ 区域的 ID 需一致
- ✧ 邻居密码认证过程需一致
- ✧ 末节区域(Stub Area)的标记需一致

DRother ←-----→ DRother Two-Way 双向状态

- OSPF 的邻接关系(Adjacencies): 建立在邻居关系之上, 交互 LSDB 信息

DR/BDR ←-----→ DRother Full 完全状态

1.2.4. OSPF包的类型

- Hello 包
- DBD (DD) 数据库的描述包
- LSR 链路状态请求包
- LSU 链路状态更新包
- LSAck LSA 确认包

1.2.5. DR和BDR的选举

- 选择接口优先级最高的为 DR
- 选择接口优先级次高的为 BDR
- 优先级为 0 的路由器不能成为 DR 或 BDR
- 如果优先级相当，则选则 Router-id 最高的
- 当网络稳定后，如果具有最高优先级的路由器，不能再成为 DR 或 BDR，除非 DR 或 BDR 故障

说明：a.选举 DR 或 BDR 的目的是为了减少重复的 LSA 通告

b. DR 和 BDR 是在一条链路上产生的，在多个子网中，可以存在多个 DR 和 BDR

OSPF 默认接口的优先级为 1 最大为 255

修改接口优先级可使用下面的命令：

```
Router(config)# interface E0/0
```

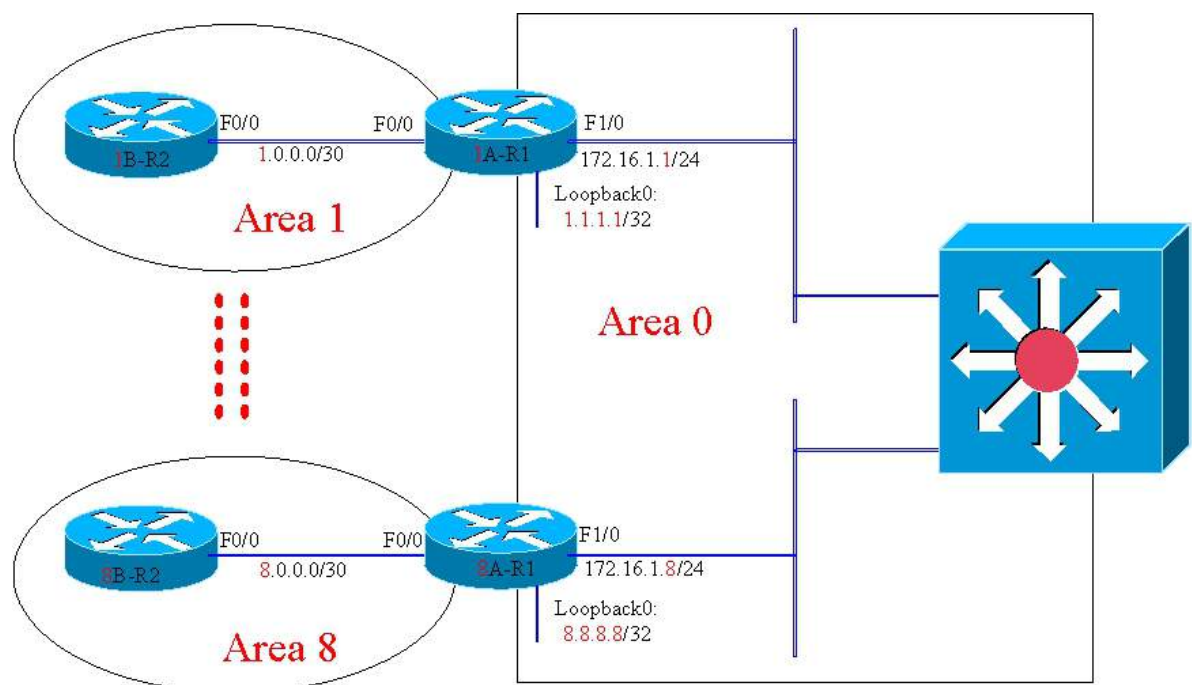
```
Router(config-if)# ip ospf priority 200
```

```
Router(config-if)# end
```

```
Router# show ip ospf interface
```

1.2.6. OSPF的实验配置

实验目的：实现多区域的 OSPF 间的路由互访，以及 DR/BDR 的选举
实验拓扑图如下：



8A-R1 配置如下：

```
8A-R1(config)# interface Loopback0
```

```
8A-R1(config-if)# ip address 8.8.8.8 255.255.255.255
```

```
8A-R1(config-if)# interface FastEthernet0/0
```

```
8A-R1(config-if)# ip address 8.0.0.1 255.255.255.252
```

```
8A-R1(config)# interface FastEthernet1/0
8A-R1(config-if)# ip address 172.16.1.8 255.255.255.0
8A-R1(config-router)# router ospf 1
8A-R1(config-router)# router-id 8.8.8.8
8A-R1(config-router)# network 8.0.0.1 0.0.0.0 area 8
8A-R1(config-router)# network 8.8.8.8 0.0.0.0 area 0
8A-R1(config-router)# network 172.16.1.8 0.0.0.0 area 0
8A-R1(config-router)# end
```

8B-R2 配置如下：

```
8A-R2(config)# interface FastEthernet0/0
8A-R2(config-if)# ip address 8.0.0.2 255.255.255.252
8A-R2(config)# router ospf 1
8A-R2(config-router)# network 8.0.0.0 0.0.0.3 area 8
8A-R2(config-router)# end
```

```
8A-R1# show ip ospf neighbor    //查看邻居信息 可查 DR/BDR/DROther 信息,优先级信息
8A-R1# show ip ospf interface    //查看当前路由器接口参与 OSPF 路由协议的详细信息
FastEthernet1/0 is up, line protocol is up
  Internet Address 172.16.1.8/24, Area 0
  Process ID 1, Router ID 8.8.8.8, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 8.8.8.8, Interface address 172.16.1.8
  Backup Designated router (ID) 3.3.3.3, Interface address 172.16.1.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

1.2.7. Router-id 的选举

在 OSPF 路由协议中，Router-id 是用来标识一台运行 OSPF 路由协议身份的自动选举规则：

- 选择 loopback 接口地址最高的
- 选择物理接口地址最高的

说明：在 OSPF 自治系统中，不允许出现重复的 Router-id，且 Router-id 的地址是可以存在，或不存在的，但建议配置 Loopback 作为一台路由器的 Router-id；如果重新修改 Router-id，请先使用 Router # clear ip ospf process 清除当前 OSPF 进程，再行修改。

1.2.8. OSPF网络类型

- Broadcast 广播的多路访问网络
- NBMA (NonBroadcast Multi Access) 非广播的多路访问网络
- Point-to-point 点到点的网络
- Point-to-Multipoint 点到多点的网络
- Point-to-Multipoint Nonbroadcast 点到多点非广播的网络

查看网络类型：

```
Router# show ip ospf interface
```

FastEthernet1/0 is up, line protocol is up

Internet Address 172.16.1.8/24, Area 0

Process ID 1, Router ID 8.7.7.7, Network Type BROADCAST, Cost: 1

修改接口的网络类型:

```
Router(config)# interface F1/0
```

```
Router(config-if)# ip ospf network point-to-point
```

```
Router(config-if)# end
```

以下描述各网络类型之间的共同点和不同点的总结:

- 每隔 10 秒发送 Hello 包的网路类型有:

Broadcast 和 Point-to-Point

说明: 以太网链路和点到点的链路是每隔 10 秒发送 Hello 包的

- 每隔 30 秒发送 Hello 包的网路类型有:

NBMA Point-to-Multipoint 和 Point-to-Multipoint Nonbroadcast

- 选举 DR 和 BDR 的网路类型的有:

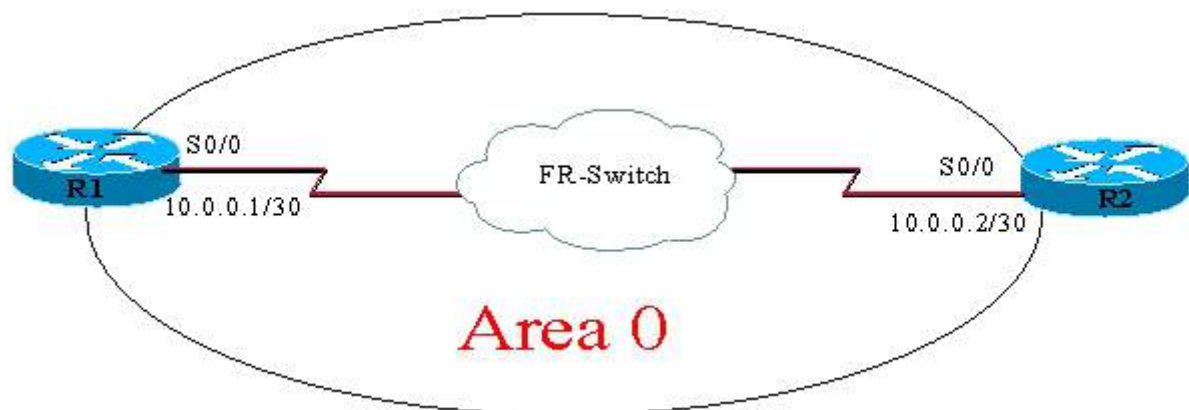
Broadcast 和 NBMA

说明: 只有多路的访问网路才会选举 DR 或 BDR

- 邻居不能够自动发现, 需手动指定邻居的网路类型有:

NBMA 和 Point-to-Multipoint Nonbroadcast

说明: 非广播的网路是不能够自动发现邻居的, 需要在一端手动指定邻居



```
8B-R2#show ip ospf interface
```

FastEthernet0/0 is up, line protocol is up

Internet Address 8.0.0.2/30, Area 8

Process ID 1, Router ID 8.0.0.2, Network Type NON_BROADCAST

```
R1(config)# router ospf 1
```

```
R1(config-router)# network 10.0.0.0 0.0.0.3 area 0
```

```
R1(config-router)# neighbor 10.0.0.2
```

```
R2(config)# router ospf 1
```

```
R2(config-router)# network 10.0.0.0 0.0.0.3 area 0
```

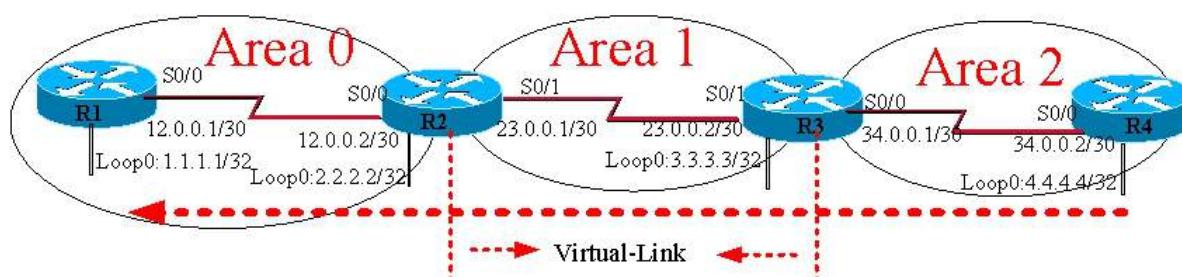
说明: Neighbor 命令可在邻居一端配置即可, 无需两端都配置

1.2.9. Virtual-Link 虚链路

作用：让常规区域的网络跨越其它的常规的区域网络跟主干区域连接，在这中间，需要配置 Virtual-Link，作虚链路连接

(前面有说明，OSPF 要求，所有的常规区域必须和主干区域相连，除非特殊情况下的临时解决方案，方可使用 Virtual-Link)

Virtual-Link 实验拓扑图



R1 的配置

```
R1(config)# interface Loopback0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config)# interface Serial0/0
R1(config-if)# ip address 12.0.0.1 255.255.255.252
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
R1(config-router)# network 12.0.0.1 0.0.0.0 area 0
R1(config-router)# end
```

R2 的配置

```
R2(config)# interface Loopback0
R2(config-if)# ip address 2.2.2.2 255.255.255.255
R2(config)# interface Serial0/0
R2(config-if)# ip address 12.0.0.2 255.255.255.252
R2(config)# interface Serial0/1
R2(config-if)# ip address 23.0.0.1 255.255.255.252
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# area 1 virtual-link 3.3.3.3
R2(config-router)# network 2.2.2.2 0.0.0.0 area 0
R2(config-router)# network 12.0.0.2 0.0.0.0 area 0
R2(config-router)# network 23.0.0.1 0.0.0.0 area 1
R2(config-router)# end
```

R3 的配置

```
R3(config)# interface Loopback0
R3(config-if)# ip address 3.3.3.3 255.255.255.255
R3(config)# interface Serial0/0
```



```

R3(config-if)# ip address 34.0.0.1 255.255.255.252
R3(config)# interface Serial0/1
R3(config-if)# ip address 23.0.0.2 255.255.255.252
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# area 1 virtual-link 2.2.2.2
R3(config-router)# network 3.3.3.3 0.0.0.0 area 1
R3(config-router)# network 23.0.0.2 0.0.0.0 area 1
R3(config-router)# network 34.0.0.1 0.0.0.0 area 2
R3(config-router)# end

```

R4 的配置

```

R4(config)# interface Loopback0
R4(config-if)# ip address 4.4.4.4 255.255.255.255
R4(config)# interface Serial0/0
R4(config-if)# ip address 34.0.0.2 255.255.255.252
R4(config)# router ospf 1
R4(config-router)# router-id 4.4.4.4
R4(config-router)# network 4.4.4.4 0.0.0.0 area 2
R4(config-router)# network 34.0.0.2 0.0.0.0 area 2
R4(config-router)# end

```

R2#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	-	23.0.0.2	OSPF_VL0
1.1.1.1	0	FULL/ -	00:00:37	12.0.0.1	Serial0/0
3.3.3.3	0	FULL/ -	00:00:37	23.0.0.2	Serial0/1

R3#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	-	23.0.0.1	OSPF_VL0
2.2.2.2	0	FULL/ -	00:00:39	23.0.0.1	Serial0/1
4.4.4.4	0	FULL/ -	00:00:31	34.0.0.2	Serial0/0

1.2.10. LSA(链路状态通知) 的类型

实验演示过程及配置请参阅下面的实验拓扑图：

➤ TYPE 1 路由器 LSA： 每台路由器都会拥有， 只会在邻居路由器之间发送

R5#show ip ospf database

Router Link States (Area 2)					
Link ID	ADV Router	Age	Seq#	Checksum	Link count
4.4.4.4	4.4.4.4	333	0x80000002	0x000BA8	1
5.5.5.5	5.5.5.5	332	0x80000003	0x006025	2

➤ TYPE 2 网络 LSA： 由所处的多路访问网络(Broadcast or NBMA)中的 DR 拥有， 只会有

DR 发出这个类型的 LSA 信息

R4#show ip ospf database

Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
45.0.0.2	5.5.5.5	470	0x80000001	0x000BCA

- TYPE 3 汇总 LSA: 由 ABR 发送, 将区域内的网络通告给 OSPF AS(自治系统)中的其它区域

R5#show ip ospf database

Summary Net Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
1.1.1.1	4.4.4.4	645	0x80000001	0x000B1A
2.2.2.2	4.4.4.4	646	0x80000001	0x00D24F
3.3.3.3	4.4.4.4	646	0x80000001	0x009A84
4.4.4.4	4.4.4.4	645	0x80000001	0x0062B9
12.0.0.0	4.4.4.4	645	0x80000001	0x0080A0
23.0.0.0	4.4.4.4	645	0x80000001	0x00E630
34.0.0.0	4.4.4.4	645	0x80000001	0x004DBF

- TYPE 4 汇总 LSA: 描述前往外部自治系统的路由信息

R5#show ip ospf database

Summary ASB Link States (Area 2)

Link ID	ADV Router	Age	Seq#	Checksum
1.1.1.1	4.4.4.4	467	0x80000001	0x00F232

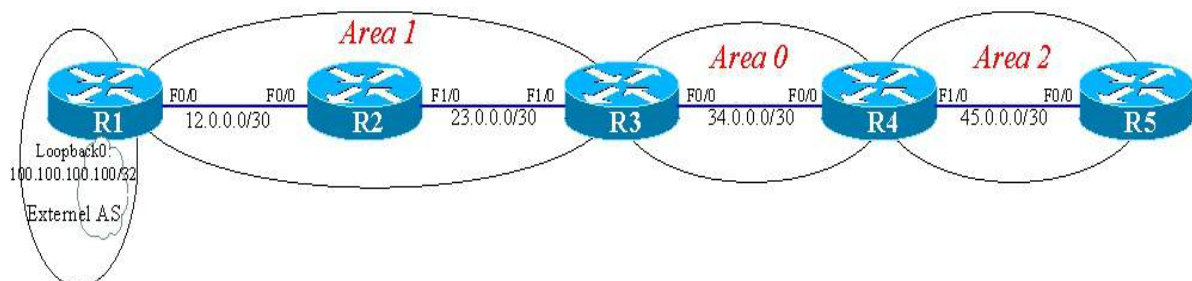
- TYPE 5 外部 LSA: 直接由 ASBR 发送, 会在整个 OSPF 的 AS 内传递

R5#show ip ospf database

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum	Tag
100.100.100.100	1.1.1.1	474	0x80000001	0x00BF4B	0

LSA 类型演示实验拓扑图



具体实现配置如下:

R1 的配置

R1(config)# interface Loopback0

R1(config-if)# ip address 1.1.1.1 255.255.255.255

R1(config-if)# ip ospf cost 100

R1(config)# interface Loopback100

R1(config-if)# ip address 100.100.100.100 255.255.255.255

```
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 12.0.0.1 255.255.255.252
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# redistribute connected metric 600 metric-type 1 subnets
R1(config-router)# network 1.1.1.1 0.0.0.0 area 1
R1(config-router)# network 12.0.0.1 0.0.0.0 area 1
R1(config-router)# end
```

R2 的配置

```
R2(config)# interface Loopback0
R2(config-if)# ip address 2.2.2.2 255.255.255.255
R2(config)# interface FastEthernet0/0
R2(config-if)# ip address 12.0.0.2 255.255.255.252
R2(config)# interface FastEthernet1/0
R2(config-if)# ip address 23.0.0.1 255.255.255.252
R2(config)# router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 2.2.2.2 0.0.0.0 area 1
R2(config-router)# network 12.0.0.2 0.0.0.0 area 1
R2(config-router)# network 23.0.0.1 0.0.0.0 area 1
R2(config-router)# end
```

R3 的配置

```
R3(config)# interface Loopback0
R3(config-if)# ip address 3.3.3.3 255.255.255.255
R3(config)# interface FastEthernet0/0
R3(config-if)# ip address 34.0.0.1 255.255.255.252
R3(config)# interface FastEthernet1/0
R3(config-if)# ip address 23.0.0.2 255.255.255.252
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 3.3.3.3 0.0.0.0 area 0
R3(config-router)# network 23.0.0.2 0.0.0.0 area 1
R3(config-router)# network 34.0.0.1 0.0.0.0 area 0
R3(config-router)# end
```

R4 的配置

```
R4(config)# interface Loopback0
R4(config-if)# ip address 4.4.4.4 255.255.255.255
R4(config)# interface FastEthernet0/0
R4(config-if)# ip address 34.0.0.2 255.255.255.252
R4(config)# interface FastEthernet1/0
R4(config-if)# ip address 45.0.0.1 255.255.255.252
R4(config)# router ospf 1
R4(config-router)# router-id 4.4.4.4
```

```
R4(config-router)# network 4.4.4.4 0.0.0.0 area 0
R4(config-router)# network 34.0.0.2 0.0.0.0 area 0
R4(config-router)# network 45.0.0.1 0.0.0.0 area 2
R4(config-router)# end
```

R5 的配置

```
R5(config)# interface Loopback0
R5(config-if)# ip address 5.5.5.5 255.255.255.255
R5(config)# interface FastEthernet0/0
R5(config-if)# ip address 45.0.0.2 255.255.255.252
R5(config)# router ospf 1
R5(config-router)# router-id 5.5.5.5
R5(config-router)# auto-cost reference-bandwidth 1000
R5(config-router)# network 5.5.5.5 0.0.0.0 area 2
R5(config-router)# network 45.0.0.2 0.0.0.0 area 2
R4(config-router)# end
```

1.2.11. 路由的类型

O 型 同一区域内的路由信息

O IA 型 同一个自治系统内区域间的路由信息

O E1 型 外部自治系统 类型 1 的路由信息

在设定的 COST 值后，传递给 OSPF 区域中时，经过的路径，会进行链路 Cost 的

累加

O E2 型 外部自治系统 类型 2 的路由信息

在设定的 COST 值后，传递给 OSPF 区域中时，不会进行累加，系统默认设置的

外部路由类型为：Type 2 (O E2)

1.2.12. 修改OSPF接口COST值和路由器的带宽值

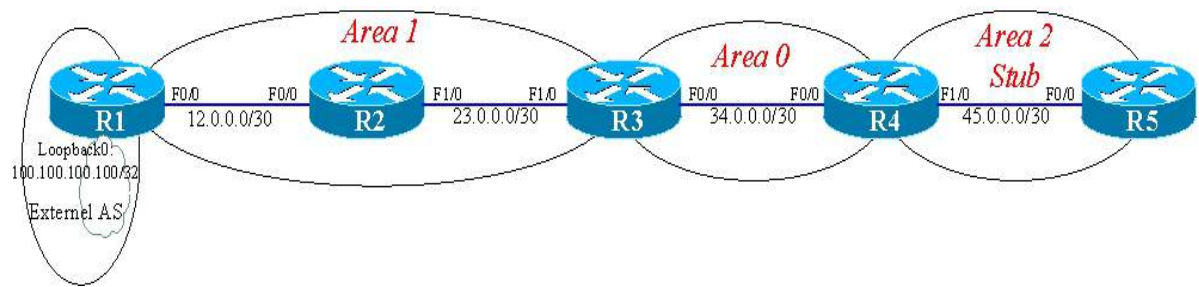
```
R1(config)# interface Loopback 0
R1(config-if)# ip ospf cost 100
R5# show ip route ospf
O IA 1.1.1.1 [110/104] via 45.0.0.1, 00:00:03, FastEthernet0/0
```

修改 OSPF 路由器的参考带宽值：默认 OSPF 路由参考带宽值为 100，每个链路的接口计算 COST 值的公式为 $100M/\text{接口带宽 } M$ ，当网络有千兆接口时，**需要全局修改**参考带宽值，要求大于或等于整个链路中的最大实际接口带宽值。

```
Router(config)#router ospf 1
Router(config-router)# auto-cost reference-bandwidth 1000 //修改为 1000M 参考带宽
```

1.2.13. OSPF的特殊区域

- Stub Area 末节区域：只接收 OSPF 自治系统区域内或区域间路由信息(LSA: 1 2 3)，不接收外部 AS 的路由信息；末节区域中，不允许拥有 ASBR 设备



R4(config)# router ospf 1

R4(config-router)# area 2 stub

R5(config)# router ospf 1

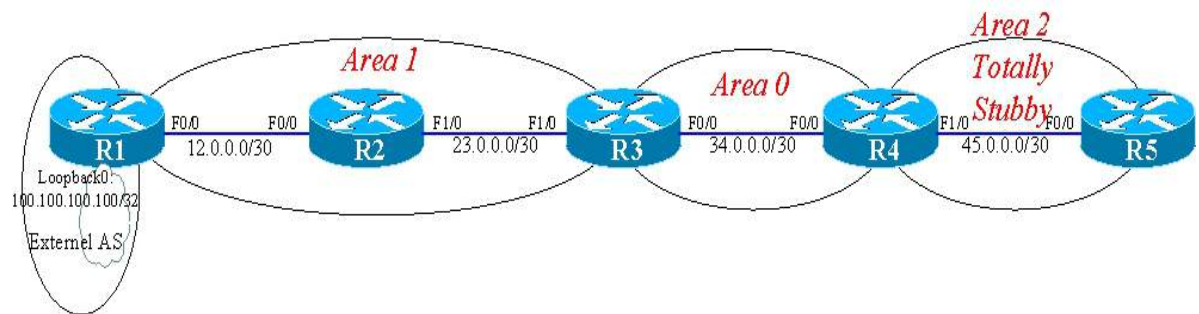
R5(config-router)# area 2 stub

R5# show ip route ospf

O*IA 0.0.0.0/0 [110/11] via 45.0.0.1, 00:01:30, FastEthernet0/0

注意： 外部路由： 100.100.100.100 已经被移除

- **Totally Stubby Area** 绝对末节区域： 只接收 OSPF 自治系统同一区域内的路由信息，不接收区域间或外部 AS 的路由信息；绝对末节区域也不允许拥有 ASBR 设备



R4(config)# router ospf 1

R4(config-router)# area 2 stub no-summary //配置绝对末节区域

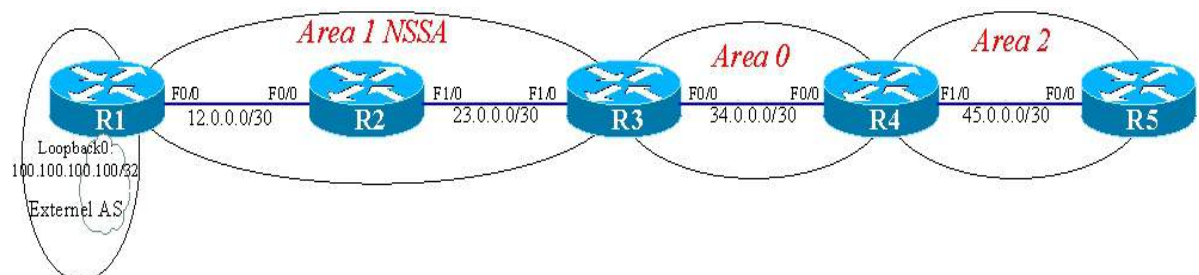
R5(config)# router ospf 1

R5(config-router)# area 2 stub

R5# show ip route

O*IA 0.0.0.0/0 [110/11] via 45.0.0.1, 00:00:58, FastEthernet0/0

- **NSSA** Not So Stubby Area 次末节区域： 具有 Stub Area 和 Totally Stubby Area 的优点，但可以含有 ASBR 设备



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

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

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

```
R3# show ip route ospf
O N1    100.100.100.100 [110/702] via 23.0.0.1, 00:03:19, FastEthernet1/0
```

```
R2# show ip route ospf
O N1    100.100.100.100 [110/701] via 12.0.0.1, 00:04:05, FastEthernet0/0
        3.0.0.0/32 is subnetted, 1 subnets
O IA    3.3.3.3 [110/2] via 23.0.0.2, 00:04:05, FastEthernet1/0
        4.0.0.0/32 is subnetted, 1 subnets
O IA    4.4.4.4 [110/3] via 23.0.0.2, 00:04:05, FastEthernet1/0
        5.0.0.0/32 is subnetted, 1 subnets
O IA    5.5.5.5 [110/4] via 23.0.0.2, 00:04:05, FastEthernet1/0
```

说明：含 O N1 和 O IA 不含有 OE1 或 OE2 路由，因为默认的 NSSA 区域是末节区域，且在 NSSA 中，默认是没有缺省路由的

如带发送缺省路由器，需做配置：

```
R3(config-router)# area 1 nssa default-information-originate
```

```
R2# show ip ospf database
```

Type-7 AS External Link States (Area 1)

Link ID	ADV Router	Age	Seq#	Checksum Tag
100.100.100.100	1.1.1.1	432	0x80000001	0x0096A0 0

```
R4# show ip route ospf
O E1    100.100.100.100 [110/703] via 34.0.0.1, 00:00:58, FastEthernet0/0
```

```
R4# show ip ospf database
```

Type-5 AS External Link States

Link ID	ADV Router	Age	Seq#	Checksum Tag
100.100.100.100	3.3.3.3	468	0x80000001	0x00EE4A 0

NSSA 的绝对末节区域

```
R3(config)# router ospf 1
R3(config-router)# area 1 nssa no-summary    //NSSA 绝对末节区域
```

```
R4(config)# router ospf 1
R4(config-router)# area 1 nssa
```

```
R5(config)# router ospf 1
```

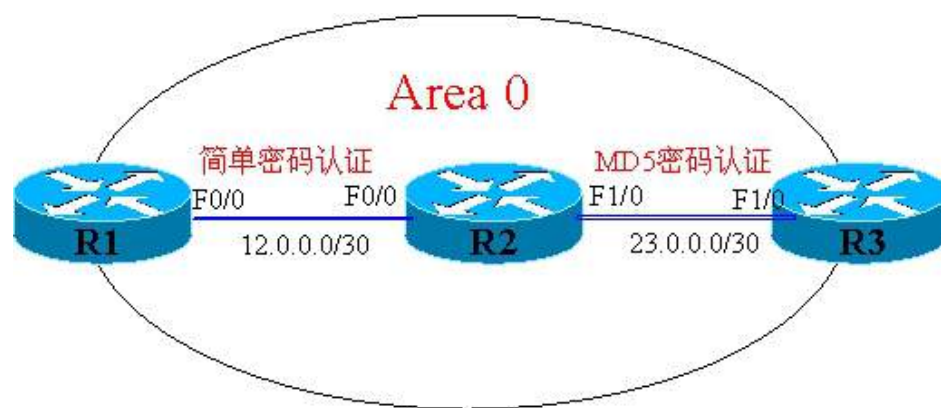
```

R5(config-router)# area 1 nssa
R2# show ip route ospf
      1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/101] via 12.0.0.1, 00:10:20, FastEthernet0/0
      100.0.0.0/32 is subnetted, 1 subnets
O N1    100.100.100.100 [110/701] via 12.0.0.1, 00:00:59, FastEthernet0/0
O*IA 0.0.0.0/0 [110/2] via 23.0.0.2, 00:01:04, FastEthernet1/0

```

1.2.14. OSPF的邻居认证

实验目的：R1 与 R2 之间使用简单密码认证，R2 与 R3 实现 MD5 密码认证
实验拓扑图如下所示：



➤ 简单密码认证配置如下：

```

R1(config)# interface f0/0
R1(config-if)# ip ospf authentication
R1(config-if)# ip ospf authentication-key cisco
R1(config-if)# end

```

```

R2(config)# interface f0/0
R2(config-if)# ip ospf authentication
R2(config-if)# ip ospf authentication-key cisco
R2(config-if)# end

```

➤ 基于 MD5 的密码认证

简单密码认证配置如下：

```

R1(config)#interface f0/0
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# ip ospf message-digest-key 1 md5 cisco
R1(config-if)# end

```

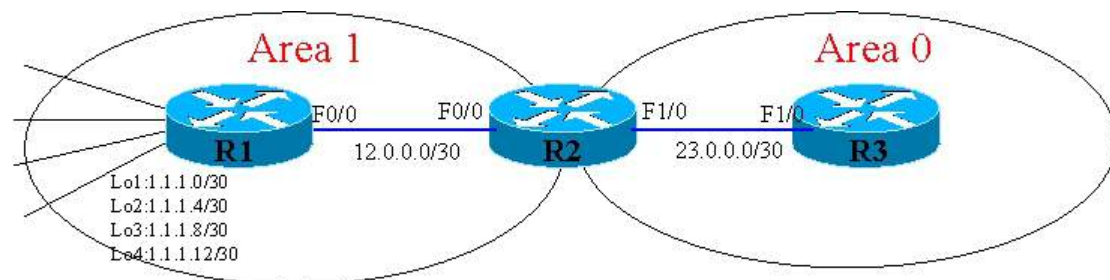
```

R2(config)#interface f0/0
R2(config-if)# ip ospf authentication message-digest
R2(config-if)# ip ospf message-digest-key 1 md5 cisco
R2(config-if)# end

```

1.2.15. OSPF的路由汇总

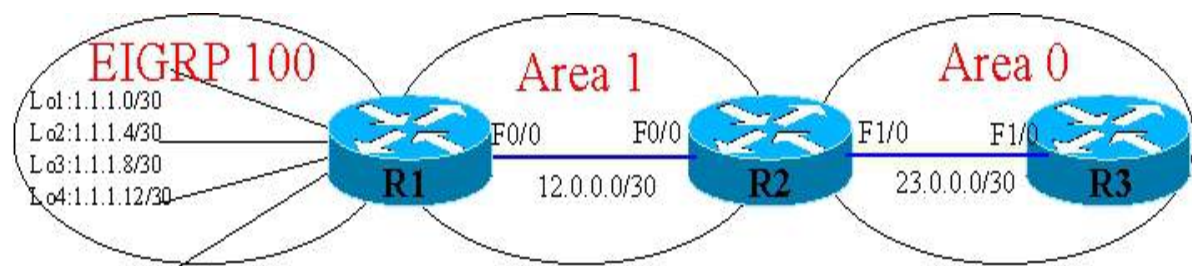
实验目的：实现在 OSPF 自治系统内区域之间的路由汇总 (在 ABR 上配置)



```
R2(config)# router ospf 1
```

```
R2(config-router)# area 1 range 1.1.1.0 255.255.255.240
```

实验目的：对外部的 OSPF 路由发布进 OSPF 时，做路由汇总(在 ASBR 上配置)



```
R1(config)# router ospf 1
```

```
R1(config-router)# summary-address 1.1.1.0 255.255.255.240
```

(操作小技巧)

```
R1(config)#no ip domain lookup //关闭 DNS 的查找
```

```
R1(config)#line console 0
```

```
R1(config-line)#logging synchronous //开启字符同步
```

```
R1(config-line)#no exec-timeout 0 //关闭 exec 模式的超时，默认为 10 分钟
```

1.3.IS-IS(中间系统) 路由协议

1.3.1. 基本概念

- IS 是指 Router (路由器)
- IS-IS 是 OSI 协议簇的一部分.
- OSI 协议簇使用无连接网络服务(CLNS)来提供数据的无连接发送
- 实际的第 3 层协议是无连接网络协议(CLNP)
- IS-IS 使用 CLNS 地址来标识路由器并建立 LSDB
- (注意: IS-IS 只支持 CLNS,而集成的 IS-IS 支持 IP 路由选择和 CLNS)

1.3.2. 相关术语

- IS 路由器
- ES 主机 HOST
- DIS 指定中间系统 (相当 OSPF 中的 DR)
- PDU 报文数据单元 (相当于 IP 报文)
- LSP 链路状态协议数据单元 (相当 OSPF 中 LSA)
- LSPDB LSP 的数据库 (相当于 OSPF 的 LSDB)
- NSAP 网络服务访问点 (相当于 IP 地址)
- IIH IS 和 IS 之间的 HELLO 包
- PSNP 部分时序协议数据单元 (相当 OSPF 的 ACK 报文)
- CSNP 全时序协议数据单元 (相当于 OSPF 的 DBD 报文)

1.3.3. 相关特性

- 属链路状态路由协议
- 集成的 ISIS 支持变长子网掩码(VLSM)
- 使用 SPF 算法计算链路，实现网络的快速收敛
- 使用 Hello 包(IIH)建立邻接关系，和使用 LSPs 交互链路状态数据信息
- 运行效能是基于：带宽、内存和处理器

1.3.4. Level-1 和 Level-2 以及 Level-1-2

- Level-1: 使用 LSPs 在本地区域建立拓扑
- Level-2: 使用 LSPs 在不同的区域之间建立拓扑
- Level-1-2: 获取本地区域内的路径和区域外的路径；相当于 OSPF 的 ABR

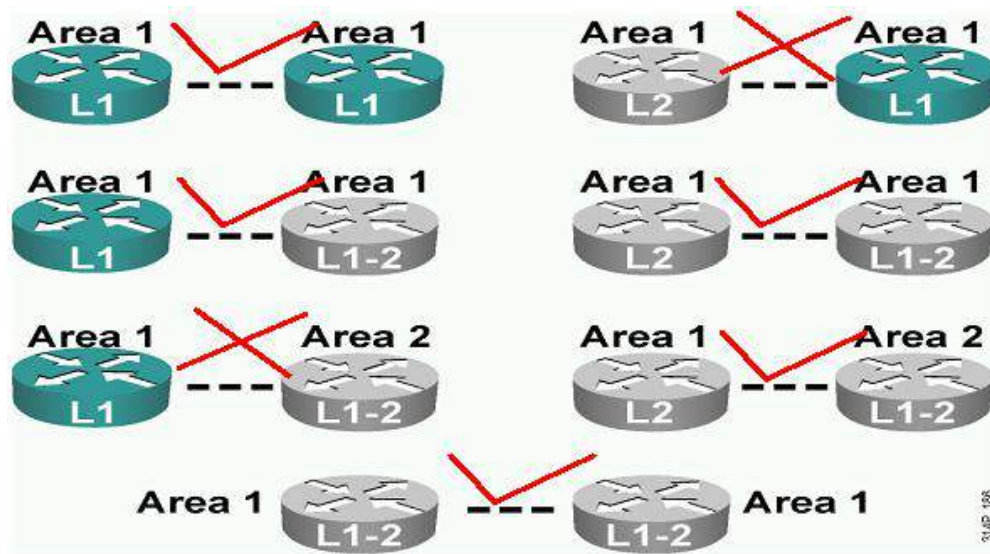
1.3.5. NSAP地址

49.0001.	1111. 1111. 1111.	00
区域 ID	系统 ID	标识

49.0001.1921.6800.2069.00

49.0001.0018.de17.d1da.00

1.3.6. IS-IS的邻居建立条件



1.3.7. 纯IS-IS的实验配置

实验目的：R1 和 R3 分别能够 ping 通各自的 NSAP 地址



纯IS-IS间通信的实验拓扑

R1 的配置

```
R1(config)# clns routing      //启用 CLNS 路由
R1(config)#router isis
R1(config-router)#net 49.0001.1111.1111.1111.00
R1(config-router)#is-type level-1
R1(config-router)#exit
R1(config)#interface s0/0
R1(config-if)#clns router isis
R1(config-if)#no shutdown
R1(config-if)#end
```

R2 的配置

```
R2(config)#clns routing
R2(config)#router isis
R2(config-router)#net 49.0001.2222.2222.2222.00
```

```
R2(config-router)#is-type level-1-2    //默认类型
R2(config-router)#exit
R2(config)#interface s0/0
R2(config-if)#clsns router isis
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0/1
R2(config-if)#clsns router isis
R2(config-if)#no shutdown
R2(config-if)#end
```

R3 的配置

```
R3(config)#clsns routing
R3(config)#router isis
R3(config-router)#net 49.0003.3333.3333.00
R3(config-router)#is-type level-2
R3(config-router)#exit
R3(config)#interface s0/1
R3(config-if)#clsns router isis
R3(config-if)#no shutdown
R3(config-if)#end
```

```
R1#ping 49.0001.2222.2222.2222.00
Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/24 ms
R1#ping 49.0003.3333.3333.3333.00
```

```
Type escape sequence to abort.
Sending 5, 100-byte CLNS Echos with timeout 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/28/44 ms
```

```
R3#show clsns route    //查看 CLNS 的路由表
Codes: C - connected, S - static, d - DecnetIV
       I - ISO-IGRP,  i - IS-IS,  e - ES-IS
       B - BGP,       b - eBGP-neighbor
```

```
C  49.0003.3333.3333.3333.00 [1/0], Local IS-IS NET
C  49.0003 [2/0], Local IS-IS Area
```

```
i  49.0001 [110/10]
   via R2, Serial0/1
```

R1#show clns neighbors //查看 CLNS 的邻居信息

System Id	Interface	SNPA	State	Holdtime	Type	Protocol
R2	Se0/0	*HDLC*	Up	26	L1	IS-IS

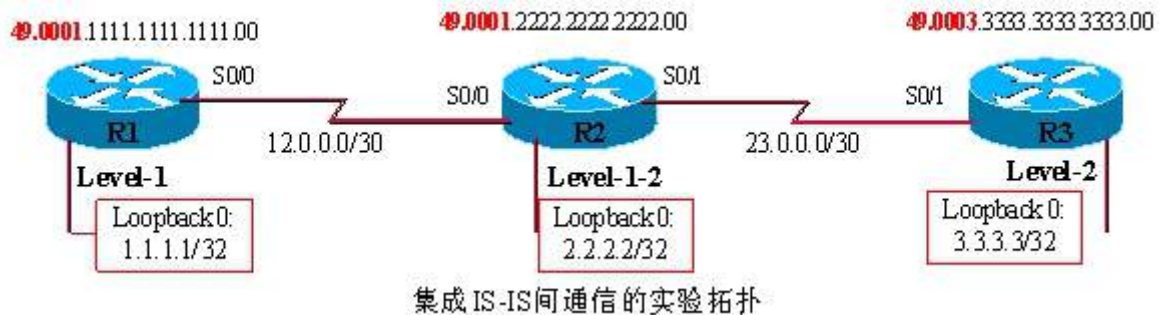
R3#show isis database //查看 IS-IS 的数据库信息

IS-IS Level-2 Link State Database:

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
R2.00-00	0x00000002	0x9767	850	0/0/0
R3.00-00	* 0x00000002	0xE318	852	0/0/0

1.3.8. 集成IS-IS的实验配置

实验目的：所有的路由器都能够 ping 通各个路由器的 Loopback 地址



R1 的配置

```
R1(config)#router isis
R1(config-router)#net 49.0001.1111.1111.1111.00
R1(config-router)#is-type level-1
R1(config-router)#exit
R1(config)#interface s0/0
R1(config-if)#ip address 12.0.0.1 255.255.255.252
R1(config-if)#ip router isis //端口启用 IP 转发
R1(config-if)#no shutdown
```

```
R1(config-if)#interface Loopback0
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#ip router isis
R1(config-if)#end
```

R2 的配置

```
R2(config)#router isis
R2(config-router)#net 49.0001.2222.2222.2222.00
R2(config-router)#exit
R2(config)#interface s0/0
R2(config-if)#ip address 12.0.0.2 255.255.255.252
R2(config-if)#ip router isis
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
R2(config)#interface s0/1
R2(config-if)#ip address 23.0.0.1 255.255.255.252
R2(config-if)#ip router isis
R2(config-if)#no shutdown
R2(config-if)#interface Loopback0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ip router isis
R2(config-if)#end
```

R3 的配置

```
R3(config)#router isis
R3(config-router)#net 49.0003.3333.3333.00
R3(config-router)#is-type level-2
R3(config-router)#exit
R3(config)#interface s0/1
R3(config-if)#ip address 23.0.0.2 255.255.255.252
R3(config-if)#ip router isis
R3(config-if)#no shutdown
R3(config-if)#interface Loopback0
R3(config-if)#ip address 3.3.3.3 255.255.255.255
R3(config-if)#ip router isis
R3(config-if)#end
```

```
R3#show ip route
      1.0.0.0/32 is subnetted, 1 subnets
i L2    1.1.1.1 [115/30] via 23.0.0.1, Serial0/1
      2.0.0.0/32 is subnetted, 1 subnets
i L2    2.2.2.2 [115/20] via 23.0.0.1, Serial0/1
      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3 is directly connected, Loopback0
      23.0.0.0/30 is subnetted, 1 subnets
C        23.0.0.0 is directly connected, Serial0/1
      12.0.0.0/30 is subnetted, 1 subnets
i L2    12.0.0.0 [115/20] via 23.0.0.1, Serial0/1
```

```
R1#show ip route
      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
i L1    2.2.2.2 [115/20] via 12.0.0.2, Serial0/0
      23.0.0.0/30 is subnetted, 1 subnets
i L1    23.0.0.0 [115/20] via 12.0.0.2, Serial0/0
      12.0.0.0/30 is subnetted, 1 subnets
C        12.0.0.0 is directly connected, Serial0/0
i*L1 0.0.0.0/0 [115/10] via 12.0.0.2, Serial0/0
```

```

R2#show ip route
    1.0.0.0/32 is subnetted, 1 subnets
i L1    1.1.1.1 [115/20] via 12.0.0.1, Serial0/0
    2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
    3.0.0.0/32 is subnetted, 1 subnets
i L2    3.3.3.3 [115/20] via 23.0.0.2, Serial0/1
    23.0.0.0/30 is subnetted, 1 subnets
C        23.0.0.0 is directly connected, Serial0/1
    12.0.0.0/30 is subnetted, 1 subnets
C        12.0.0.0 is directly connected, Serial0/0

```

IS-IS 的路由汇总

```

R2(config)# router isis
R2(config-router)# summary-address 1.1.1.0 255.255.255.0 level-1-2
R2#show ip route
    1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
i su    1.1.1.0/24 [115/20] via 0.0.0.0, Null0

```

```

R3# show ip route
    1.0.0.0/24 is subnetted, 1 subnets
i L2    1.1.1.0 [115/30] via 23.0.0.1, Serial0/1

```

1.4.BGP 边界网关协议

IGP (内部网关协议) : RIPv1 RIPv2 IGRP EIGRP OSPF ISIS

EGP(外部网关协议) : BGP

1.4.1. 何时使用BGP

- AS(自主系统)允许分组(数据)穿过它前往其它自主系统（例如，服务提供商）
- AS 有多条到其它自主系统的连接
- 必须对数据流进入和离开 AS 的方式进行控制

1.4.2. 满足以下条件之一时，不要使用BGP

- 只有一条到 Internet 或另一个 AS 的连接
- 路由器没有足够的内存和处理器能力来处理 BGP 的更新
- 对路由过滤和 BGP 路径选择过程的了解有限
- 自主系统之间的链路的带宽较低

1.4.3. BGP的特性

- BGP 是一个路径矢量协议，在距离矢量路由协议上增进以下的功能：
- 可靠的更新，运行和结束使用 TCP(port 179)
- 触发更新时，发送增量更新
- 周期性的保持信息和校验 TCP 的连接性
- 有充足的距离矢量的属性值(为选择路径而用的)
- 设计的对象是一个巨大的互联网网络
- 建立 BGP 的邻居条件为：TCP 可达。

1.4.4. BGP的数据库

- 邻居表：列出所有 BGP 的邻居
Router# show ip bgp neighbor //查看 BGP 的邻居
- BGP 表(转发数据库):
Router# show ip bgp //查看 BGP 表
 - a.列出从每个邻居学习到所有网络的信息
 - b.包含多条路径到达目标网络
 - c.每个路径都包含 BGP 的属性
- IP 路由表 (又称为 IGP 表): 列出最佳的路径到达目标网络
Router# show ip route

1.4.5. BGP的消息类型

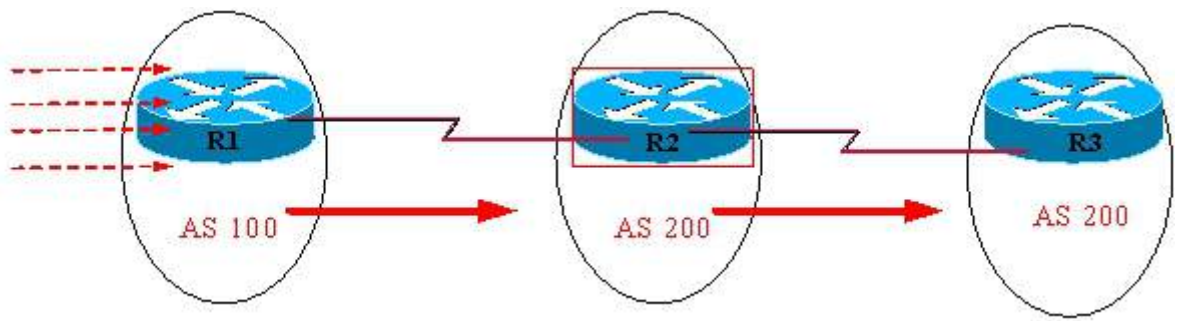
- Open 打开消息
- Keepalive 存活消息
- Update 更新消息
- Notification 通知消息

1.4.6. 关于IBGP与EBGP之间的关系

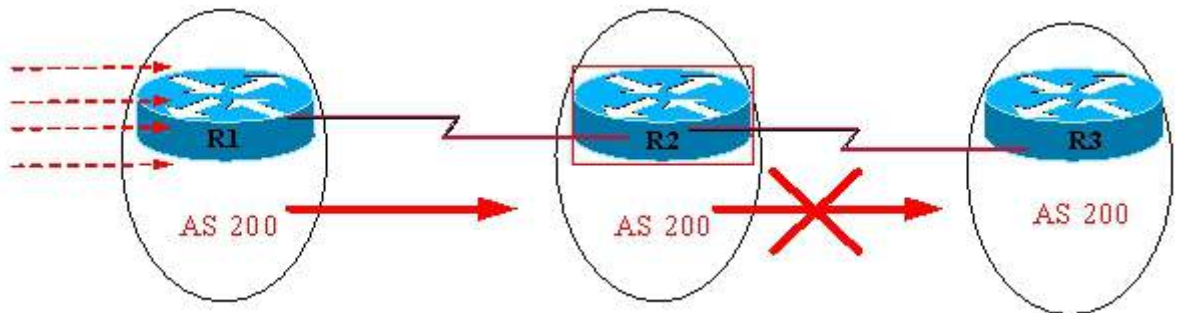
- IBGP: 在同一个 AS 之内设备之间建立的邻居关系
- EBGP: 在不同的 AS 之间建立的邻居关系
- 说明: 建立 BGP 邻居的首要条件为：TCP 可达

下列图例将说明各 BGP 邻居之间的传递关系

- 1、由 EBGP 邻居学来的信息会传递给 IBGP 邻居



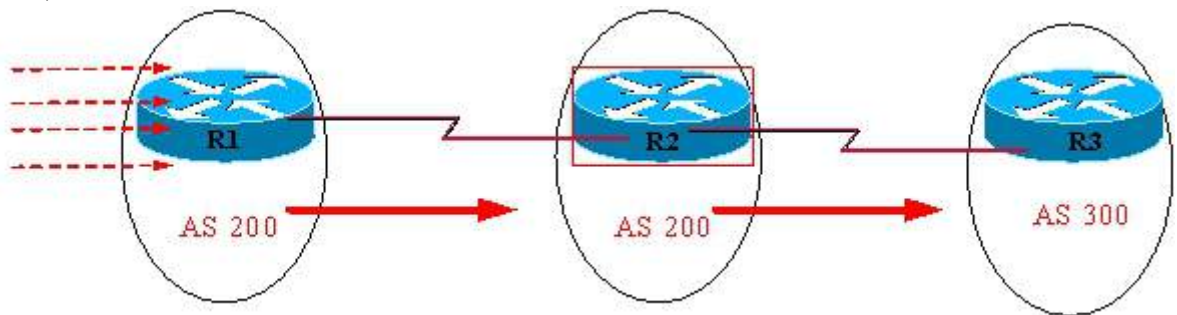
2、由 IBGP 邻居学来的信息，不会传递给另外的 IBGP 邻居



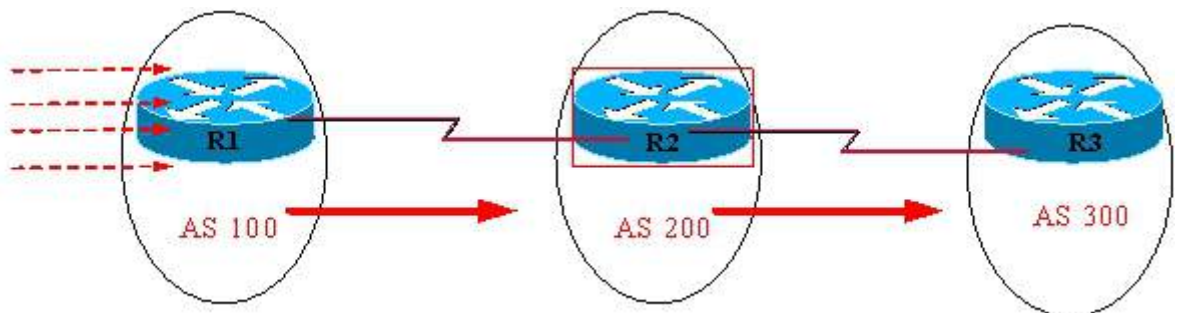
3、由 IBGP 邻居学来的信息：

A: 如果在 R2 上同步关闭，则会将信息传递给 EBGP 邻居 R3(后期 IOS 版本的路由器默认为同步关闭状态)

B: 如果在 R2 上同步开启，则不会传递给 EBGP 邻居(原因为：BGP 要求，从 IBGP 邻居学来的路由信息理应不传递给 EBGP 邻居，因为直接从 IBGP 邻居学来的路由信息并不一定是可达的路由)



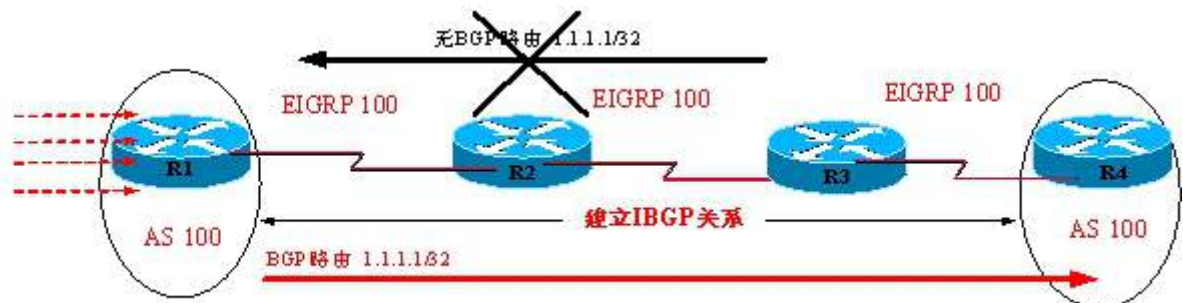
4、由 EBGP 邻居学来的信息，会传递给其它的 EBGP 邻居



5、BGP 路由传递过程中出现的路由黑洞现象

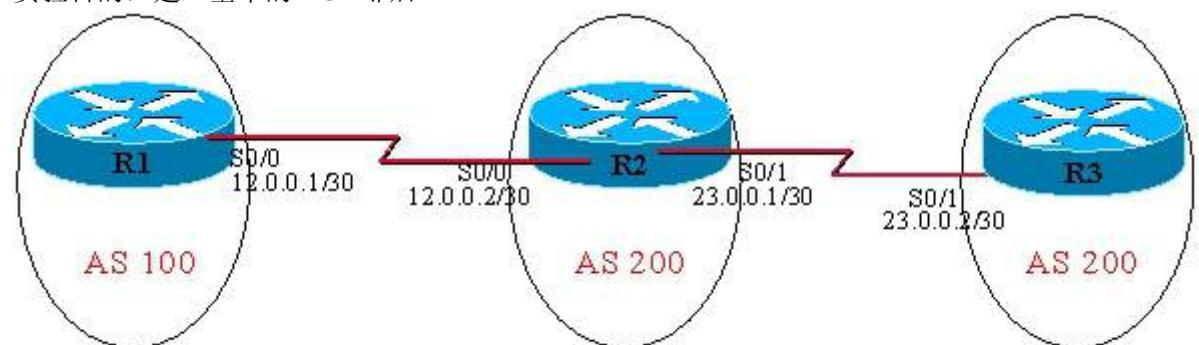
R1 与 R4 建立了 IBGP 的邻居关系，R1 的 BGP 路由信息，根据路由的传递规则，将会通过 TCP

分组方式直接传递给 R4，R4 在收到 R1 发送过来的报文后，解开数据包，然后将相应的数据信息加入 BGP 表或 IGP 表；当 R4 试图访问 R1 之前发过来的路由时，则根据路由的逐跳转发规则，将会把数据送达给下一跳路由器 R3，但是 R3 没有参与过 BGP 的建立，所以，路由表中不可能有前往 R1 的 BGP 路由，所以 R3 将请求数据包给丢弃，这就形成了 BGP 的路由黑洞。(解决方法可以使用 MPLS 或将 BGP 路由重分发进 IGP 中)



1.4.7. 基本BGP邻居建立的实验

实验目的：建立基本的 BGP 邻居



```
R1(config)#router bgp 100
R1(config-router)#neighbor 12.0.0.2 remote-as 200
R1(config-router)#end
```

```
R2(config)#router bgp 200
R2(config-router)#neighbor 12.0.0.1 remote-as 100
R2(config-router)#neighbor 23.0.0.2 remote-as 200
R2(config-router)#end
```

R2#show ip bgp summary //查看 BGP 邻居的汇总信息

BGP router identifier 23.0.0.1, local AS number 200

BGP table version is 1, main routing table version 1

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
12.0.0.1	4	100	4	4	0	0	0	00:01:04	0
23.0.0.2	4	200	0	0	0	0	0	never	Active

说明：邻居表中的 23.0.0.2 状态为：never 状态，所以，邻居未建立。

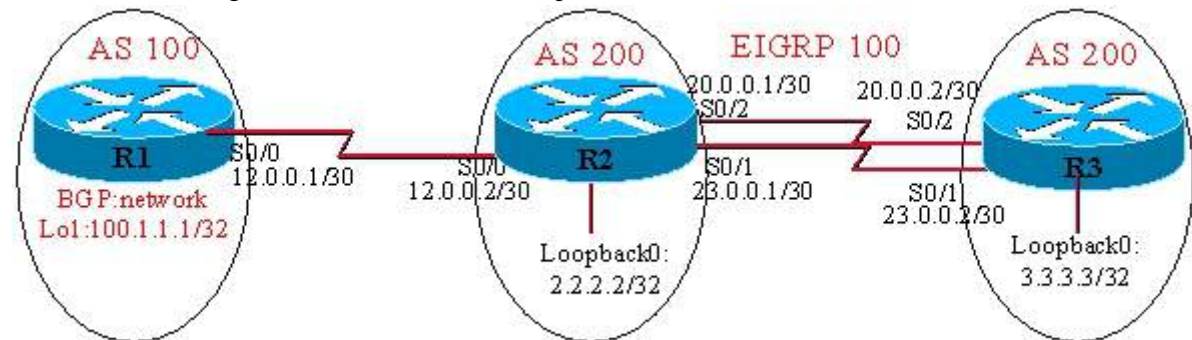
```
R3(config)#router bgp 200
R3(config-router)#neighbor 23.0.0.1 remote-as 200
```

```
R3(config-router)#end
```

1.4.8. 高级的BGP(属性)实验

1、Update-Source 更新源

BGP 建议：在建立 IBGP 邻居时，使用 Loopback 地址作为 Update-Source(更新源)，但在建立邻居时，也需使用 Neighbor 命令指定对端的 Loopback 接口地址



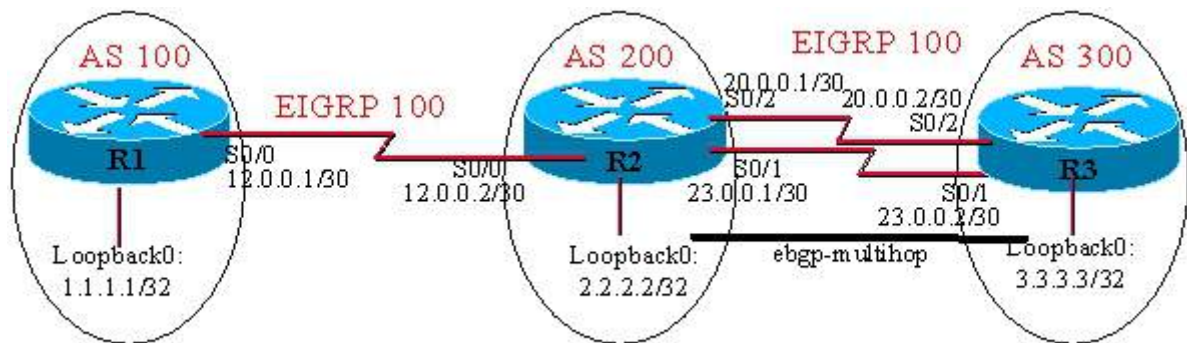
删除原来 R2 与 R3 之间建立直连链路的 BGP 邻居

```
R2(config)#interface loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#exit
R2(config)# router eigrp 10
R2(config-router)# no auto-summary
R2(config-router)# network 20.0.0.0
R2(config-router)# network 23.0.0.0
R2(config-router)# network 2.0.0.0
R2(config)#router bgp 200
R2(config-router)#neighbor 3.3.3.3 remote-as 200
R2(config-router)#neighbor 3.3.3.3 update-source loopback 0
R2(config-router)#end
```

```
R3(config)#interface loopback 0
R3(config-if)#ip address 3.3.3.3 255.255.255.255
R3(config-if)#exit
R3(config)# router eigrp 10
R3(config-router)# no auto-summary
R3(config-router)# network 20.0.0.0
R3(config-router)# network 23.0.0.0
R3(config-router)# network 3.0.0.0
R3(config)#router bgp 200
R3(config-router)#neighbor 2.2.2.2 remote-as 200
R3(config-router)#neighbor 2.2.2.2 update-source loopback 0
R3(config-router)#end
```

2、EBGP-Multihop ebgp 多跳

BGP 要求，默认情况下，ebgp 之间邻居关系的建立，只能为直连链路，若跨越多个子网段，则需要使用 ebgp 多跳功能来指定 ebgp 邻居，最大支持 255 条

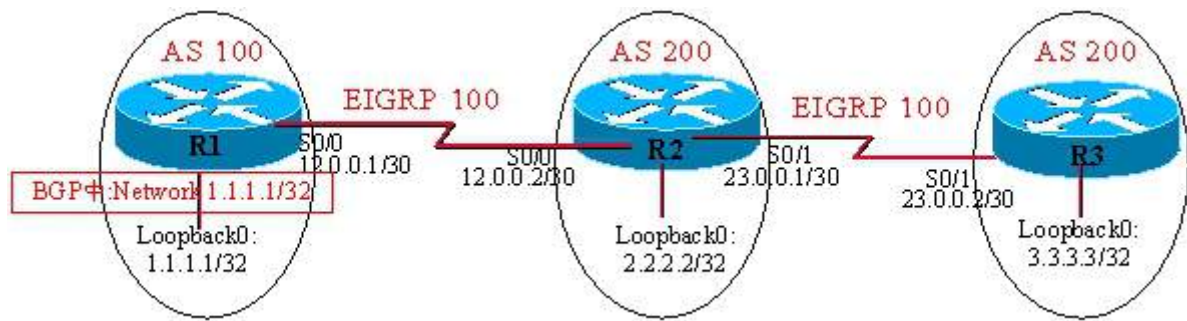


```
R2(config)#router eigrp 100
R2(config-router)# no auto-summary
R2(config-router)# network 20.0.0.0
R2(config-router)# network 23.0.0.0
R2(config-router)# network 2.0.0.0
R2(config)#router bgp 200
R2(config-router)#neighbor 3.3.3.3 remote-as 300
R2(config-router)#neighbor 3.3.3.3 update-source loopback 0
R2(config-router)#neighbor 3.3.3.3 ebgp-multihop 2
R2(config-router)#end
```

```
R3(config)#router eigrp 100
R3(config-router)# no auto-summary
R3(config-router)# network 20.0.0.0
R3(config-router)# network 23.0.0.0
R3(config-router)# network 3.0.0.0
R3(config)#router bgp 300
R3(config-router)#neighbor 2.2.2.2 remote-as 200
R3(config-router)#neighbor 2.2.2.2 update-source loopback 0
R3(config-router)#neighbor 2.2.2.2 ebgp-multihop 2
R3(config-router)#end
```

3、Next-hop-self 下一跳自我

在 BGP 中所说的下一跳，是指下一跳 AS，而并非是下一跳路由器
由 EBGP 学来的路由信息，在传递给 IBGP 邻居时，不改变其下一跳属性值



```
R1(config)#router bgp 100
R1(config-router)# network 1.1.1.1 mask 255.255.255.255
R1(config-router)# end
```

```
R2#show ip bgp
Network          Next Hop          Metric LocPrf Weight Path
r> 1.1.1.1/32     1.1.1.1           0              0 100 i
```

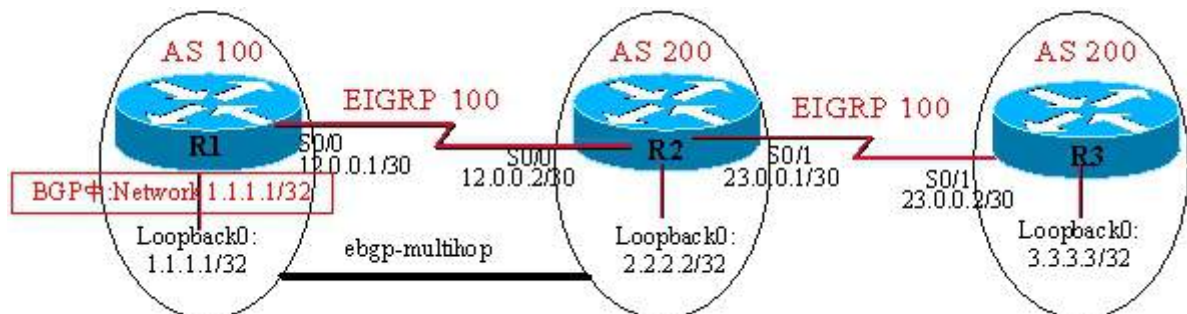
```
R3#show ip bgp
Network          Next Hop          Metric LocPrf Weight Path
* i1.1.1.1/32     1.1.1.1           0    100      0 100 i
```

```
R2(config)# router bgp 200
R2(config-router)# neighbor 3.3.3.3 next-hop-self
R2(config-router)# end
```

```
R3#show ip bgp
Network          Next Hop          Metric LocPrf Weight Path
*>i1.1.1.1/32     2.2.2.2           0    100      0 100 i
```

说明： *> 表示有效且最佳的

4、BGP 的邻居验证



说明： 分别配置 R1 和 R2 之间做邻居验证，R2 与 R3 之间做邻居验证

```
R1(config)# router bgp 100
R1(config-router)# neighbor 2.2.2.2 password cisco123
```

```
R2(config)#router bgp 200
```

```
R2(config-router)# neighbor 1.1.1.1 password cisco123
```

```
R2(config-router)# neighbor 3.3.3.3 password cisco
```

```
R3(config)#router bgp 200
```

```
R3(config-router)# neighbor 2.2.2.2 password cisco
```

```
R2# clear ip bgp * //清除当前所有邻居，重新建立邻居
```

```
R2# clear ip bgp 3.3.3.3
```

1.4.9. BGP的路径属性

➤ 公认属性：所有 BGP 实现都必须能够识别的属性。这些属性被传输给 BGP 邻居

公认强制属性：必须出现在 BGP 的更新中；As path(AS 路径)、Next-hop(下一跳)、Origin(起源)

公认自决属性：可以不出现在 BGP 更新中；如 Local preference(本地优先级属性)

➤ 可选属性：非公认属性被称为是可选的，可选属性是可以传递或非传递的，实现了可选属性的 BGP 路由器可能根据其含义将其传播给 BGP 邻居；

➤ 思科私有属性：Weight 权重属性，本地配置，只在本地有效，不会传播给其它的 BGP 邻居路由器。在 Cisco 路由器上面，优先级是最高的

1.4.10. BGP路由选择决策过程

对于特定的目的地，BGP 只选择一条最佳路径

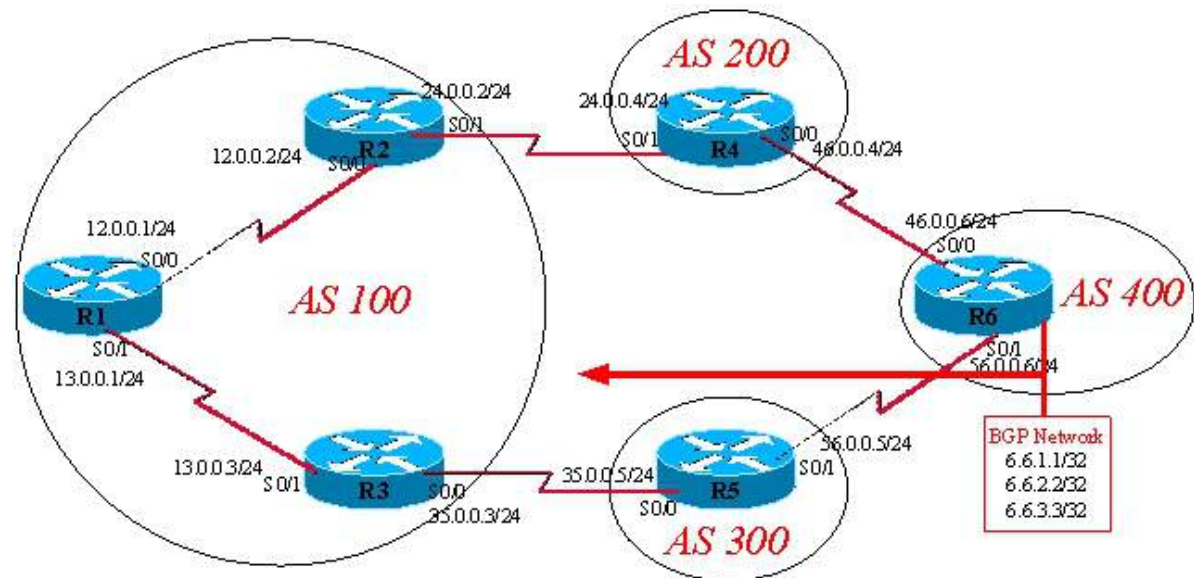
如果到达目标有多条路径，则将会依据以下这些策略进行路径选择

- 1、选权重最高的路由(属 cisco 私有属性，只在当前本地路由器有效)
- 2、选择本地优先级最高的路由(注：只用于本地 AS 内部)
- 3、选择当前路由器的通告过的路由
- 4、选择 AS 路径最短的路由
- 5、选择源头编码最小的路径(依次为 IGP<EGP<Incomplete)
- 6、选择 MED 值最小的路径
- 7、外部路径(EBGP)优先于内部路径(IGP)
- 8、选择经过最近的 IGP 邻居的路径
- 9、对于 EBGP 路径，选择最老的路由
- 10、选邻居 BGP 路由器 ID 最小的路由
- 11、选择邻居 IP 地址最小的路由

说明：只有最佳的路由才会被加入到 BGP 表中，并被传播给 BGP 邻居

1.4.11. 使用 Route-map 操纵 BGP 路径实验 (Local_prefence As-path)

实验目的：利用 Route-map 工具实验操纵改变 BGP 的转发路径



R1 的基本配置

```
R1(config)# interface Serial0/0
R1(config-if)# ip address 12.0.0.1 255.255.255.0
R1(config)# interface Serial0/1
R1(config-if)# ip address 13.0.0.1 255.255.255.0
R1(config)# router bgp 100
R1(config-router)# neighbor 12.0.0.2 remote-as 100
R1(config-router)# neighbor 13.0.0.3 remote-as 100
R1(config-router)# end
```

R2 的基本配置

```
R2(config)# interface Serial0/0
R2(config-if)# ip address 12.0.0.2 255.255.255.0
R2(config)# interface Serial0/1
R2(config-if)# ip address 24.0.0.2 255.255.255.0
R2(config)# router bgp 100
R2(config-router)# neighbor 12.0.0.1 remote-as 100
R2(config-router)# neighbor 12.0.0.1 next-hop-self
R2(config-router)# neighbor 24.0.0.4 remote-as 200
R2(config-router)# end
```


R3 的基本配置

```
R3(config)# interface Serial0/0
R3(config-if)# ip address 35.0.0.3 255.255.255.0
R3(config)# interface Serial0/1
R3(config-if)# ip address 13.0.0.3 255.255.255.0
R3(config-router)# router bgp 100
R3(config-router)# neighbor 13.0.0.1 remote-as 100
R3(config-router)# neighbor 13.0.0.1 next-hop-self
R3(config-router)# neighbor 35.0.0.5 remote-as 300
R3(config-router)# end
```

R4 的基本配置

```
R4(config)# interface Serial0/0
R4(config-if)# ip address 46.0.0.4 255.255.255.0
R4(config)# interface Serial0/1
R4(config-if)# ip address 24.0.0.4 255.255.255.0
R4(config)# router bgp 200
R4(config-router)# neighbor 24.0.0.2 remote-as 100
R4(config-router)# neighbor 46.0.0.6 remote-as 400
R4(config-router)# end
```

R5 的基本配置

```
R5(config)# interface Serial0/0
R5(config-if)# ip address 35.0.0.5 255.255.255.0
R5(config)# interface Serial0/1
R5(config-if)# ip address 56.0.0.5 255.255.255.0
R5(config)# router bgp 300
R5(config-router)# no synchronization
R5(config-router)# neighbor 35.0.0.3 remote-as 100
R5(config-router)# neighbor 56.0.0.6 remote-as 400
R5(config-router)# end
```

R6 的基本配置

```
R6(config)# interface Loopback1
R6(config-if)# ip address 6.6.1.1 255.255.255.255
R6(config)# interface Loopback2
R6(config-if)# ip address 6.6.2.2 255.255.255.255
R6(config)# interface Loopback3
R6(config-if)# ip address 6.6.3.3 255.255.255.255
R6(config)# interface Serial0/0
R6(config-if)# ip address 46.0.0.6 255.255.255.0
R6(config)# interface Serial0/1
R6(config-if)# ip address 56.0.0.6 255.255.255.0
R6(config)# router bgp 400
R6(config-router)# network 6.6.1.1 mask 255.255.255.255
R6(config-router)# network 6.6.2.2 mask 255.255.255.255
```

```

R6(config-router)# network 6.6.3.3 mask 255.255.255.255
R6(config-router)# neighbor 46.0.0.4 remote-as 200
R6(config-router)# neighbor 56.0.0.5 remote-as 300
R6(config-router)# end

```

R3 使用 Local_preference 改变路径

```

R3(config)# router bgp 100
R3(config-router)# neighbor 35.0.0.5 route-map LOCAL_PRE in
R3(config)# access-list 33 permit 6.6.3.3
R3(config)# route-map LOCAL_PRE permit 10
R3(config-route-map)# match ip address 33
R3(config-route-map)# set local-preference 333
R3(config)# route-map LOCAL_PRE permit 20
R3(config-route-map)# set as-path prepend 111 112 113 114 115
R3(config-route-map)# end

```



R1 查看结果

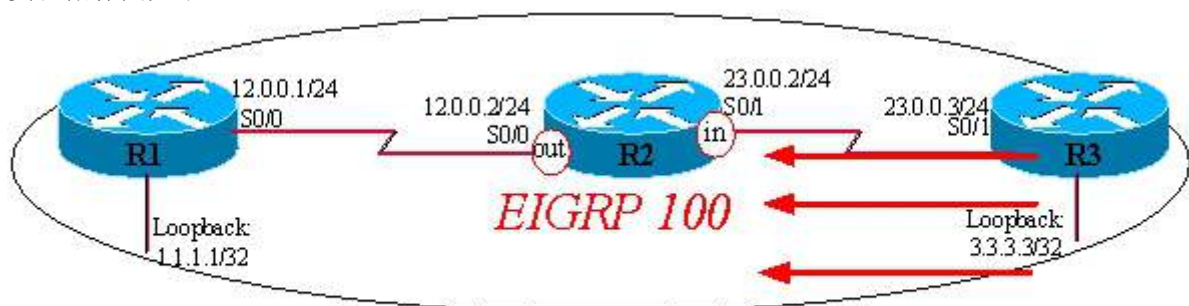
```
R1#show ip bgp
```

Network	Next Hop	Metric	LocPrf	Weight	Path
* i6.6.1.1/32	13.0.0.3	0	100	0	111 112 113 114 115 300 400 i
*>i	12.0.0.2	0	100	0	200 400 i
* i6.6.2.2/32	13.0.0.3	0	100	0	111 112 113 114 115 300 400 i
*>i	12.0.0.2	0	100	0	200 400 i
*>i6.6.3.3/32	13.0.0.3	0	333	0	300 400 i
* i	12.0.0.2	0	100	0	200 400 i

1.5. 过滤路由的更新

实验目的：使用 Distribute- List (分发列表)实现路由过滤

实验拓扑图如下：



R2 的实验配置

```

R2(config)# router eigrp 100
R2(config-router)# network 12.0.0.0
R2(config-router)# network 23.0.0.0

```

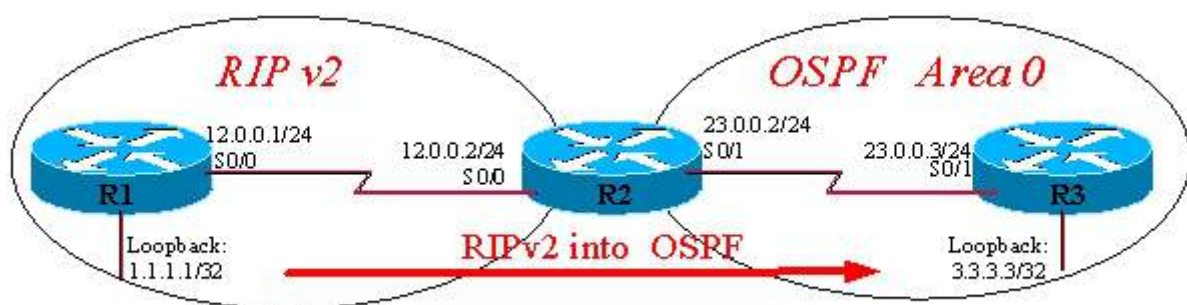


```
R2(config-router)# distribute-list 19 in Serial0/1 或 (distribute-list 19 out Serial0/0)
R2(config-router)# no auto-summary
R2(config-router)# end
R2(config)# access-list 19 permit 23.0.0.0 0.0.0.255
```

1.6. 路由重分发(Redistribution)

作用：将一个路由协议的路由重分发进另一个路由协议中，实现多路由协议的互相通信

1.6.1. 将RIPv2路由重分发进 OSPF 中

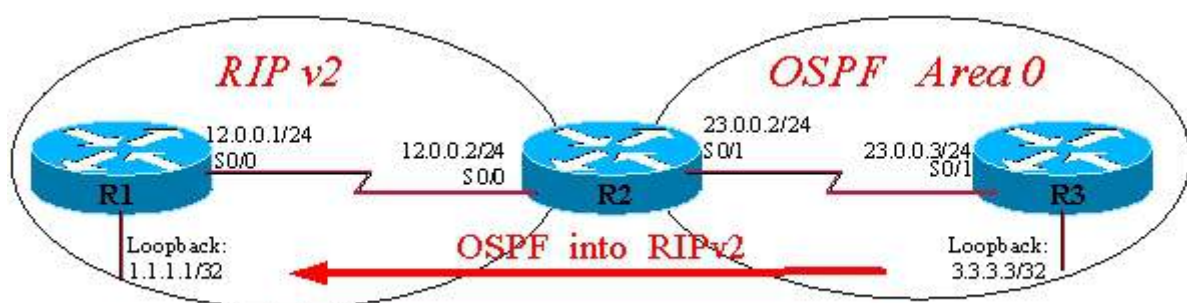


在 ASBR 上配置路由重分发

```
R2(config)# router ospf 1
R2(config-router)# redistribute rip metric 10 metric-type 2 subnets
```

```
R3#show ip route ospf
      1.0.0.0/32 is subnetted, 1 subnets
O E2    1.1.1.1 [110/10] via 23.0.0.2, 00:05:20, Serial0/1
      12.0.0.0/24 is subnetted, 1 subnets
O E2    12.0.0.0 [110/10] via 23.0.0.2, 00:05:20, Serial0/1
```

1.6.2. 将OSPF路由重分发进RIPv2中



```
R2(config)# router rip
R2(config-router)# redistribute ospf 1 metric 3
```

```

R1#show ip route rip
R    3.0.0.0/8 [120/3] via 12.0.0.2, 00:00:22, Serial0/0
R    23.0.0.0/8 [120/3] via 12.0.0.2, 00:00:22, Serial0/0

```

1.6.3. 将EIGRP 100 重分发进OSPF 中



```

R2(config)#router ospf 1
R2(config-router)# redistribute eigrp 100 metric 10 subnets

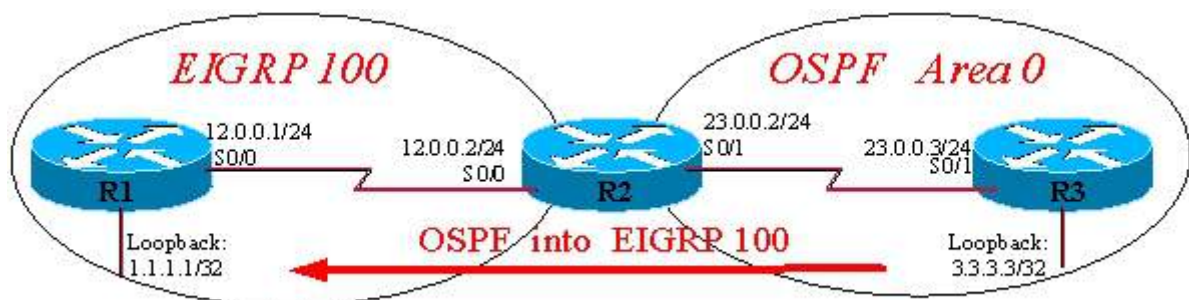
```

```

R3#show ip route ospf
    1.0.0.0/32 is subnetted, 1 subnets
O E2    1.1.1.1 [110/10] via 23.0.0.2, 00:00:05, Serial0/1
    12.0.0.0/24 is subnetted, 1 subnets
O E2    12.0.0.0 [110/10] via 23.0.0.2, 00:00:05, Serial0/1

```

1.6.4. 将OSPF重分发进EIGRP 100 中



```

R2(config-router)# router eigrp 100
R2(config-router)# redistribute ospf 1 metric 100000 1000 255 1 1500

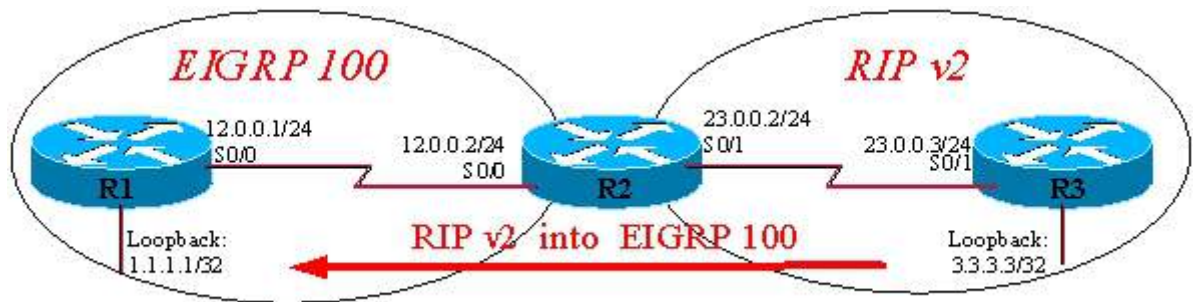
```

```

R1#show ip route eigrp
    3.0.0.0/32 is subnetted, 1 subnets
D EX    3.3.3.3 [170/2425856] via 12.0.0.2, 00:00:44, Serial0/0
    23.0.0.0/24 is subnetted, 1 subnets
D EX    23.0.0.0 [170/2425856] via 12.0.0.2, 00:00:44, Serial0/0

```

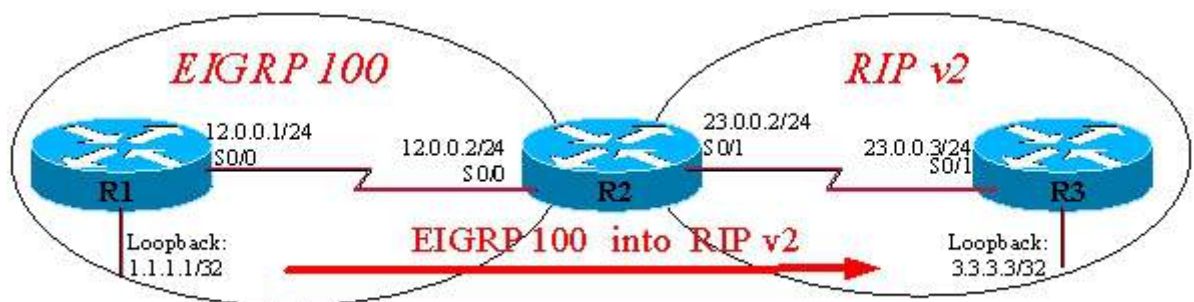
1.6.5. 将RIP v2 重分发进EIGRP 100 中



```
R2(config)# router eigrp 100
```

```
R2(config-router)# redistribute rip metric 100000 1000 255 1 1500
```

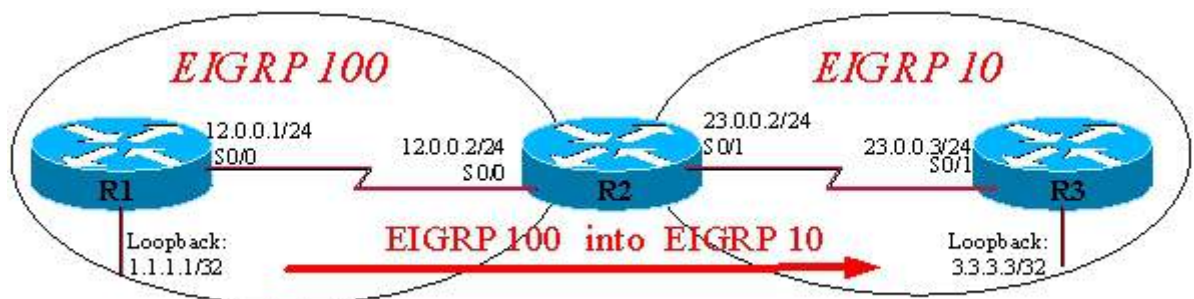
1.6.6. 将EIGRP 100 重分发进 RIPv2 中



```
R2(config)# router rip
```

```
R2(config-router)# redistribute eigrp 100 metric 3
```

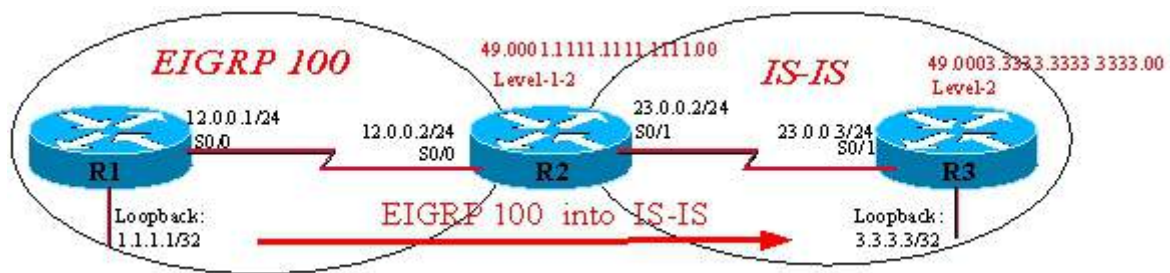
1.6.7. 将EIGRP 100 重分发进 EIGRP 10



```
R2(config)#router eigrp 10
```

```
R2(config-router)# redistribute eigrp 100
```

1.6.8. 将EIGRP 100 重分发进 集成ISIS中



//以下配置为基本配置，其中省略了接口 IP 地址的配置

```
R2(config)#router isis
```

```
R2(config-router)# net 49.0001.1111.1111.1111.00
```

```
R2(config-router)# exit
```

```
R2(config)# interface s0/1
```

```
R2(config-if)# ip router isis
```

```
R3(config)#router isis
```

```
R3(config-router)# is-type level-2
```

```
R3(config-router)# net 49.0003.3333.3333.3333.00
```

```
R3(config-router)# interface s0/1
```

```
R3(config-if)#ip router isis
```

```
R3(config-if)#interface loopback0
```

```
R3(config-if)#ip router isis
```

//开始配置重分发

```
R2(config)#router isis
```

```
R2(config-router)# redistribute eigrp 100 level-1-2
```

```
R3# show ip route isis
```

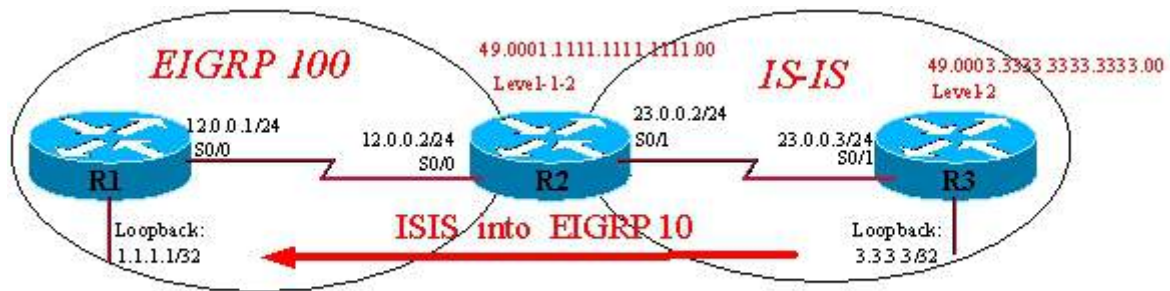
```
1.0.0.0/32 is subnetted, 1 subnets
```

```
i L2    1.1.1.1 [115/10] via 23.0.0.2, Serial0/1
```

```
12.0.0.0/24 is subnetted, 1 subnets
```

```
i L2    12.0.0.0 [115/10] via 23.0.0.2, Serial0/1
```

1.6.9. 将ISIS 重分发进EIGRP 100



```
R2(config)#router eigrp 100
```

```
R2(config-router)# redistribute isis metric 1000000 1000 255 1 1500
```

```
R2(config-router)# redistribute connected //重分发直连
```

说明：关于 Redistribute Connected 命令的功能：将当前所有未通过路由协议命令发布出去的接口，直接发布进当前进程中的路由协议

```
R1# show ip route eigrp
```

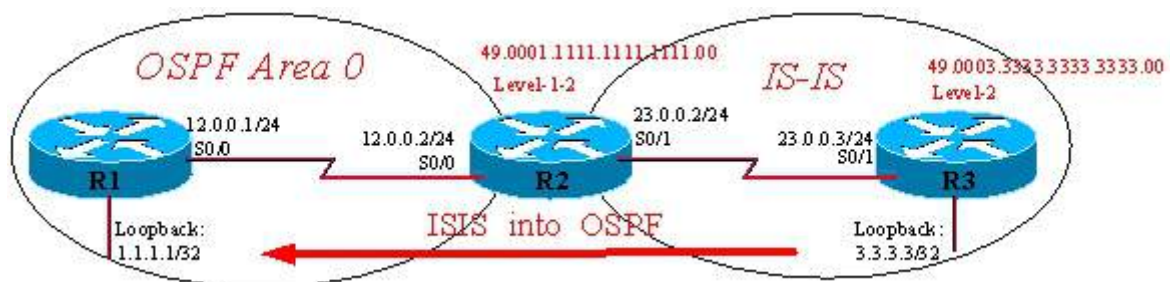
```
3.0.0.0/32 is subnetted, 1 subnets
```

```
D EX    3.3.3.3 [170/2425856] via 12.0.0.2, 00:08:02, Serial0/0
```

```
23.0.0.0/24 is subnetted, 1 subnets
```

```
D EX    23.0.0.0 [170/2681856] via 12.0.0.2, 00:06:36, Serial0/0
```

1.6.10. 将ISIS重发分进OSPF中



```
R2(config)# router ospf 1
```

```
R2(config-router)# redistribute isis metric 100 subnets
```

```
R2(config-router)# redistribute connected subnets
```

```
R1# show ip route ospf
```

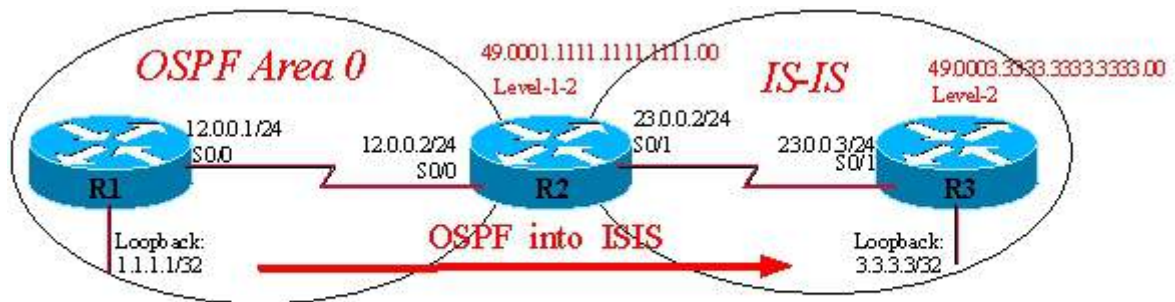
```
3.0.0.0/32 is subnetted, 1 subnets
```

```
O E2    3.3.3.3 [110/100] via 12.0.0.2, 00:01:07, Serial0/0
```

```
23.0.0.0/24 is subnetted, 1 subnets
```

```
O E2    23.0.0.0 [110/20] via 12.0.0.2, 00:00:18, Serial0/0
```


1.6.11. 将OSPF 重分发进ISIS中



```
R2(config)# router isis
```

```
R2(config-router)# redistribute ospf 1 level-1-2
```

```
R3#show ip route isis
```

```
1.0.0.0/32 is subnetted, 1 subnets
```

```
i L2 1.1.1.1 [115/10] via 23.0.0.2, Serial0/1
```

```
12.0.0.0/24 is subnetted, 1 subnets
```

```
i L2 12.0.0.0 [115/10] via 23.0.0.2, Serial0/1
```

1.7. 各种路由协议的管理距离值

➤ Connected interface (直连接口)	0
➤ Static route	1
➤ EIGRP summary route	5
➤ External BGP	20
➤ Internal EIGRP	90
➤ IGRP	100
➤ OSPF	110
➤ IS-IS	115
➤ RIPv1,RIPv2	120
➤ External EIGRP	170
➤ Internal BGP	200
➤ Unknown	255

1.8.(MultiCast)组播

单播(Unicast)、广播(Broadcast)与组播(Multicast)的区别

当前的 IPv4 网络中有三种通讯模式：单播、广播、组播，其中的组播出现时间最晚，但同时具备单播和广播的优点，最具有发展前景。

1.8.1. 单播数据流

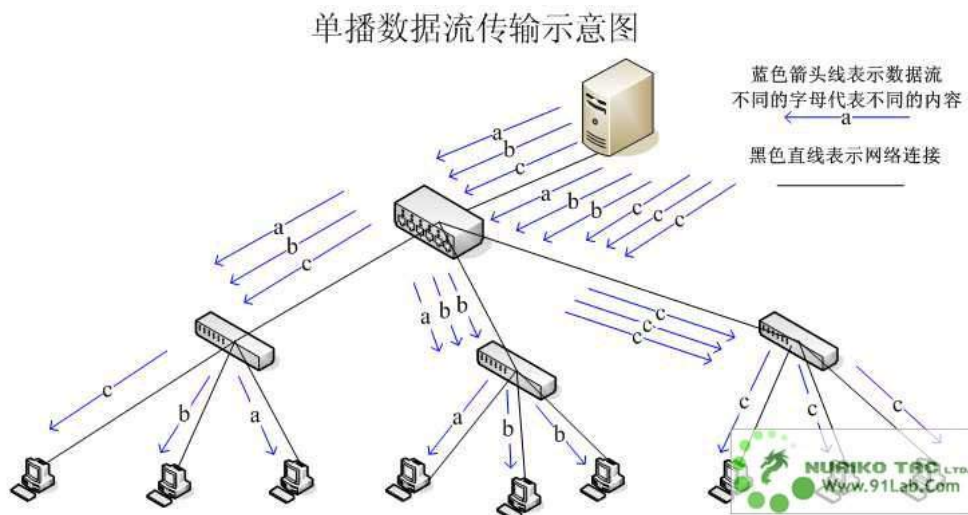
主机之间“一对一”的通讯模式。网络中的交换机和路由器对数据只进行转发不进行复制。如果 10 个客户机需要相同的数据，则服务器需要逐一传送，重复 10 次相同的工作。但由于其能够针对每个客户的及时响应，所以现在的网页浏览全部都是采用单播协议。网络中的路由器和交换机根据其目标地址选择传输路径，将 IP 单播数据传送到其指定的目的地。

单播的优点：

- 服务器及时响应客户机的请求
- 服务器针对每个客户不同的请求发送不同的数据，容易实现个性化服务。

单播的缺点：

- 服务器针对每个客户机发送数据流，服务器流量=客户机数量×客户机流量；在客户数量大、每个客户机流量大的流媒体应用中服务器不堪重负。
- 现有的网络带宽是金字塔结构，城际省际主干带宽仅仅相当于其所有用户带宽之和的 5%。如果全部使用单播协议，将造成网络主干不堪重负。现在的 P2P 应用就已经使主干经常阻塞，只要有 5% 的客户在全速使用网络，其他人就不要玩了。而将主干扩展 20 倍几乎是不可能。



1.8.2. 广播数据流

主机之间“一对所有”的通讯模式，网络对其中每一台主机发出的信号都进行无条件复制并转发，所有主机都可以接收到所有信息（不管你是否需要），由于其不用路径选择，所以其网络成本可以很低廉。有线电视网就是典型的广播型网络，我们的电视机实际上是接受到所有频道的信号，但只将一个频道的信号还原成画面。在数据网络中也允许广播的存在，但其被限制在二层交

换机的局域网范围内，禁止广播数据穿过路由器，防止广播数据影响大面积的主机。

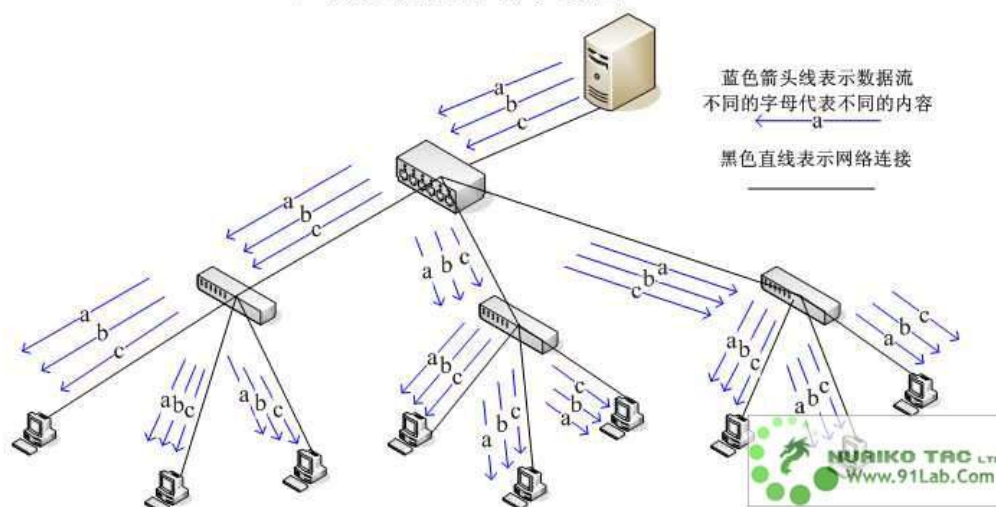
广播的优点：

- 网络设备简单，维护简单，布网成本低廉
- 由于服务器不用向每个客户机单独发送数据，所以服务器流量负载极低。

广播的缺点：

- 无法针对每个客户的要求和时间及时提供个性化服务。
- 网络允许服务器提供数据的带宽有限，客户端的最大带宽=服务总带宽。例如有线电视的客户端的线路支持 100 个频道（如果采用数字压缩技术，理论上可以提供 500 个频道），即使服务商有更大的财力配置更多的发送设备、改成光纤主干，也无法超过此极限。也就是说无法向众多客户提供更多样化、更加个性化的服务。
- 广播禁止在 Internet 宽带网上传输。

广播数据流传输示意图



1.8.3. 组播数据流

主机之间“一对一组”的通讯模式，也就是加入了同一个组的主机可以接受到此组内的所有数据，网络中的交换机和路由器只向有需求者复制并转发其所需数据。主机可以向路由器请求加入或退出某个组，网络中的路由器和交换机有选择的复制并传输数据，即只将组内数据传输给那些加入组的主机。这样既能一次将数据传输给多个有需要（加入组）的主机，又能保证不影响其他不需要（未加入组）的主机的其他通讯。

组播的优点：

- 需要相同数据流的客户端加入相同的组共享一条数据流，节省了服务器的负载。具备广播所具备的优点。
- 由于组播协议是根据接受者的需要对数据流进行复制转发，所以服务端的服务总带宽不受客户接入端带宽的限制。IP 协议允许有 2 亿 6 千多万个（268435456）组播，所以其提供的服务可以非常丰富。
- 此协议和单播协议一样允许在 Internet 宽带网上传输。

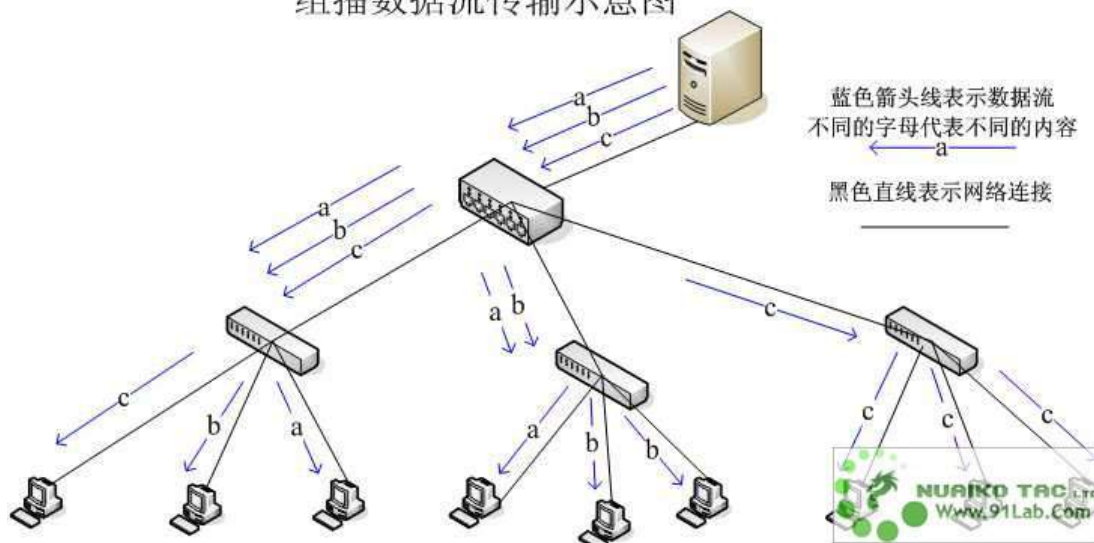
1.8.4. 组播的缺点：

- 与单播协议相比没有纠错机制，发生丢包错包后难以弥补，但可以通过一定的容错机制和 QOS

加以弥补。

- 现行网络虽然都支持组播的传输，但在客户认证、QOS 等方面还需要完善，这些缺点在理论上都有成熟的解决方案，只是需要逐步推广应用到现存网络当中

组播数据流传输示意图



1.8.5. IP的组播地址(3 层地址)

D 类地址范围 224.0.0.0 – 239.255.255.255

1、保留地址范围：

- 224.0.0.1: 所有支持组播的主机
- 224.0.0.2: 所有支持组播的路由器
- 224.0.0.5: OSPF 路由协议
- 224.0.0.6: OSPF 路由协议
- 224.0.0.9: RIPv2 路由协议
- 224.0.0.10: EIGRP 路由协议
- 224.0.0.13 PIMv2 路由器

2、全局组播地址：

范围：224.0.1.0 到 238.255.255.255

3、MBONE(组播骨干网地址)

范围：224.2.0.0 到 224.2.255.255

4、私有组播地址：

范围：239.0.0.0/8 地址段

1.8.6. 数据链路层的 2 层组播地址

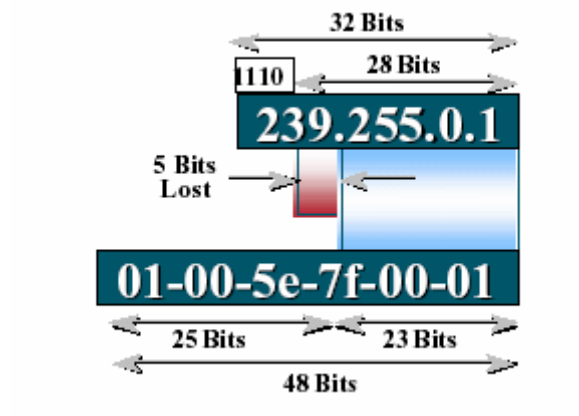
三层组播地址前四个二进制位固定为 1110，所以后面共有 28 位可变。

MAC 地址一共 48 位，分 6 节，前面三节为 01-00-5E 的专门用于与三层多播地址建立映射。

且第四节的首位固定为 0，所以 MAC 地址中有 23 位可变。

我们就是把组播地址的后 23 位映射到 MAC 地址的后 23 位上。

没错，映射时漏掉了 28 位可变组播地址的前 5 位。



1.8.7.IGMP互联网组管理协议

1、IGMPv1：版本 1 采用路由器查询和主机报告两种方法维护组成员关系。

路由器向 224.0.0.1（all hosts）地址发送 TTL=1 的查询包，这种查询每 60-120s 发生一次，如果在一个 LAN 上面存在多台路由器，则只有其中的一台作为 Designated/Elected 的路由器发送查询信息。

2、IGMPv2：对版本 1 的改良主要体现在以下几个方面：

在原有的发向 224.0.0.1 的针对所有组成员关系的 General Query 的基础上增加发向特定组地址的针对特定组的查询，以确定是否仍存在该组的接收者。

当主机离开一个组时，主动向路由器发送注销报告，当发送此报告的主机是最后一个组成员时，可以减少路由器停止特定组播消息前的延时。

版本 2 中关于 Designated Router 的选举有了固定的机制，单播地址最小的支持 IGMP 协议的路由器成为 Query Router。

此外，路由器在发出查询包时可以指定主机响应时间间隔。

3、IGMPv3：主要的变化是在原有的组播记录中增加了针对组播源的列表，用来记录接收者接受或拒绝的源。这样就决定了要想利用版本 3 的新特性，路由器和主机内的 IGMP 协议以及基于组播的应用程序都要更新。

基本查看命令：

1、查看 IGMP 的接口信息及版本号

```
Router>show ip igmp interface e0
```

```
Ethernet0 is up, line protocol is up
```

```
Internet address is 1.1.1.1, subnet mask is 255.255.255.0
```

```
IGMP is enabled on interface
```

```
Current IGMP version is 2
```

2、查看 IGMP 组成员信息

```
Router> show ip igmp group
```

1.8.8. 第 2 层组播帧交换

用于映射多播地址的 MAC 地址段 01-00-5E 是专用的，这样的 MAC 地址不会出现在源地址中，所以交换机不可能学习到关于组播的交换条目，默认的情况下，交换机处理组播帧的方式和广播帧一样，在一个广播域内泛洪传播。

当然，我们可以通过手工添加静态表项来解决这一问题，但是组播的接收者是动态变化的，静态的映射方式往往不能反映主机的真实要求。

好的方法是动态建立转发映射，但是交换机没有能力知道第三层的事，无法对组播的转发做出准确判断。如何解决这一难题呢？下面我们介绍几种方法。

1、IGMP snooping (IGMP 嗅探)

让交换机也懂 IGMP？没错，就是这个意思，交换机在监听主机和路由器之间的 IGMP 会话，但这样做意味着交换机必须复制并分析所有的组播帧才能找寻出所有的 IGMP 数据包。可以想像这是一项繁重的任务，会严重影响交换机的性能，用专用芯片来实现这一处理过程可以释解交换机的压力，但同时会增加交换机的成本。

2、CGMP(思科组管理协议)

CGMP 以 Client/Server 方式工作，路由器相当于服务器，交换机相当于客户机，路由器接收到 IGMP 消息后，以 CGMP 指令通知交换机多播接收者加入或退出多播组的情况，指导交换机进行准确的多播定向转发。

1.8.9. 组播路由协议

1、组播分布树(分发树：源树和共享树)

SPT Shortest Path Tree (最短路径树)

对于组播中的每个信源，都将为其创建一个源树。源树的根为组播的源，其分支经过网络到达各个接收方。源树也被称为源路由树或最短路径树，因为它从信源前往接收方时采用的是路径最短。组播路由的状态为：(S, G) S 表示：Source 源 G 表示：Group 组

运行路由协议为：PIM Dense Mode 密集模式

SDT Shared Distribution Tree (共享分布树)

共享树是组播组的所有信源之间共享的一个分发树。共享树的根被称为汇聚点(RP)。信源只将组播数据流发送给 RP，RP 再通过共享树将其转发给组播组的成员。

组播路由的状态为：(*, G) *表示：任意的 source 源 G 表示：Group 组

必须含有 Rendezvous Point (RP) 汇聚点

运行路由协议为：PIM Sparse Mode 稀疏模式

2、组播的路由类型

PIM（协议无关多播）是允许在现有的 IP 网络上增加 IP 多播路由选择的体系结构。可以在两种模式下运行

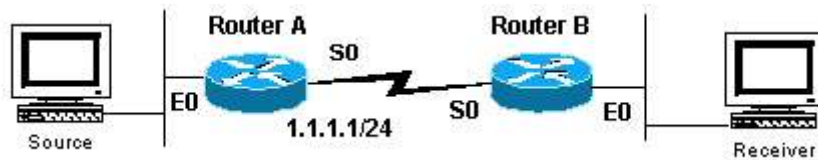
1、DM (Dense Mode)密集模式

在整个网络中泛洪组播数据包，然后进行链路修剪，可以得出从源到接收者之间的一个最短路径；组播路由协议会每隔 3 分钟对整个链路进行泛洪和修剪

2、SM (Sparse Mode)稀疏模式

在网络中设定一个或多个 RP(汇聚点), 所有的加入请求都会将指向 RP; 其中 RP 可以通过手动方式进行配置, 也可以自动配置

1.8.10. 带有RP的稀疏密集的实验配置



路由器 A 的配置

```
RouterA(config)# ip multicast-routing
RouterA(config)# ip pim rp-address 1.1.1.1
RouterA(config)# interface E0
RouterA(config-if)# ip address 192.168.1.1 255.255.255.0
RouterA(config-if)# ip pim sparse-dense-mode
RouterA(config-if)# no shutdown
RouterA(config-if)# interface S0
RouterA(config-if)# ip address 1.1.1.1 255.255.255.252
RouterA(config-if)# ip pim sparse-dense-mode
RouterA(config-if)# no shutdown
```

路由器 B 的配置

```
RouterB(config)# ip multicast-routing
RouterB(config)# ip pim rp-address 1.1.1.1
RouterB(config)# interface E0
RouterB(config-if)# ip address 192.168.2.1 255.255.255.0
RouterB(config-if)# ip pim sparse-dense-mode
RouterB(config-if)# no shutdown
RouterB(config-if)# interface S0
RouterB(config-if)# ip address 1.1.1.2 255.255.255.252
RouterB(config-if)# ip pim sparse-dense-mode
RouterB(config-if)# no shutdown
```

1.9. IPV6

1.9.1. IPV6 的特性

- 拥有巨大的地址空间
- 改善了全球可达性和灵活性
- 能够在路由选择表中聚合通告的前缀

- 自动配置链路层的地址，从而实现即插即用的功能
- 无需进行网络地址转换(NAT)就能进行端到端的通信
- 路由的转发效率得到了提高
- 简化了重新编址和修改地址的机制
- 性能和转发速度也得到了很好的提升
- 没有广播（使用任意播代替）
- 增加了扩展的头部：流标签
- IPv4 到 IPv6 的地址过渡：双栈技术、6to4 的隧道技术

1.9.2. 地址空间

IPv4 32 bits or 4 bytes

4,200,000,000 possible addressable nodes 4.2×10^9

IPv6 128 bits or 16 byte

3.4×10^{38} possible addressable nodes

340,282,366,920,938,463,374,607,432,768,211,456

5×10^{28} addresses per person

1.9.3. IPv6 的地址格式

- IPv6 地址是由 128 位 2 进制数组成的，共分 8 节，每节 16 位，用 16 进制数表示
- 每一节地址之间使用冒号“：”隔开，如：X:X:X:X:X:X:X:X
- 0031:0000:130F:0000:0000:09C0:876A:130B/64
- 简化：31:0:130F::9c0:876A:130B/64

说明：如遇连续的多个 0，可使用双冒号代替::，在一个地址中，只允许使用一个双冒号

2001::A001/96 相当于 2001:0000:0000:0000:0000:0000:0000:A001/96

2001:0000:0000:0000:AAAA:0000:00000:0001/64 简化：

2001::AAAA:0:0:1/64 2001:0:0:0:AAA::1/64

2001::B001:0:0:1/64 2001:0:0:0:B001::1/64

公司地址使用示例

2001::A001:1/112

2001::B001:1/112

2001::C001:1/112

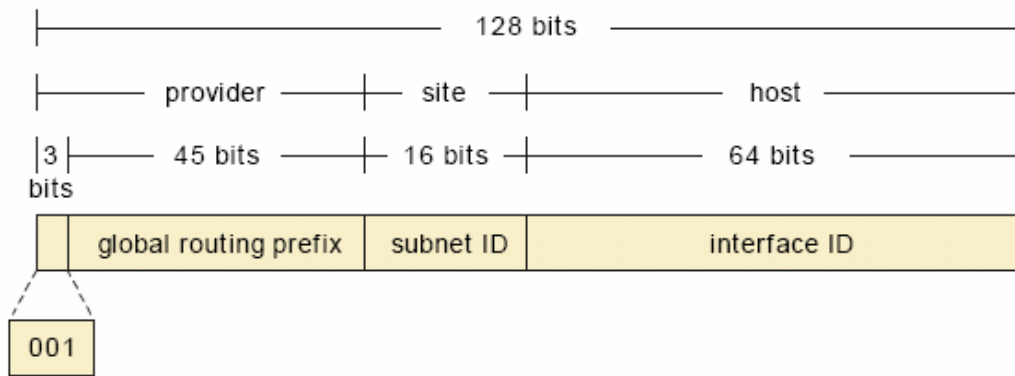
2001::D001:1/112

1.9.4. IPv6 地址类型

- 单播地址 UniCast

用于确认单独接口的一个地址。发往单播地址的数据包被发送到该地址所确认的接口。按照数据包的可达性，单播支持以下类型的地址：

全局单播地址。能够全球到达和确认的地址。全局单播地址由一个全局选路前缀、一个子网 ID 和一个接口 ID 组成(如图所示)。当前全局单播地址分配使用的地址范围从二进制值 001 (2000::/3) 开始，即全部 IPv6 地址空间的八分之一。



- 站点本地单播地址。只能在客户站点内到达和确认的地址，类似于 IPv4 专用地址 10.0.0.0/8 和 192.168.0.0/16。站点本地单播地址包含一个 FEC0::/10 前缀、子网 ID 以及接口 ID（如图所示）。

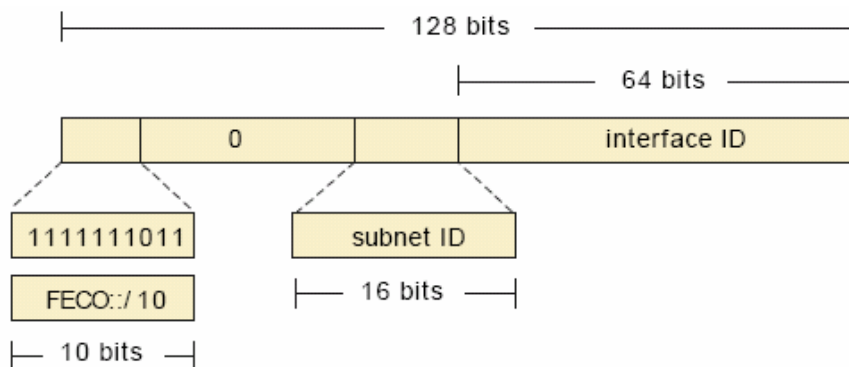


图 4. 站点本地单播地址格式

- 链路本地单播地址。只能由与同一本地链路相连的节点到达和确认的地址。链路本地单播地址使用 FE80::/10 前缀和一个接口 ID

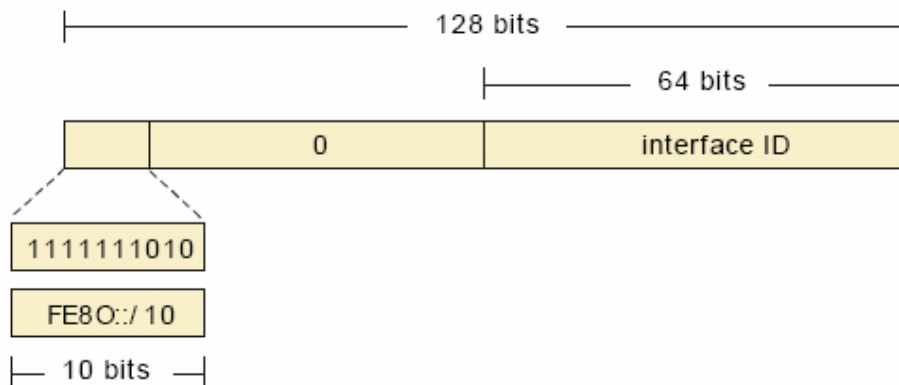
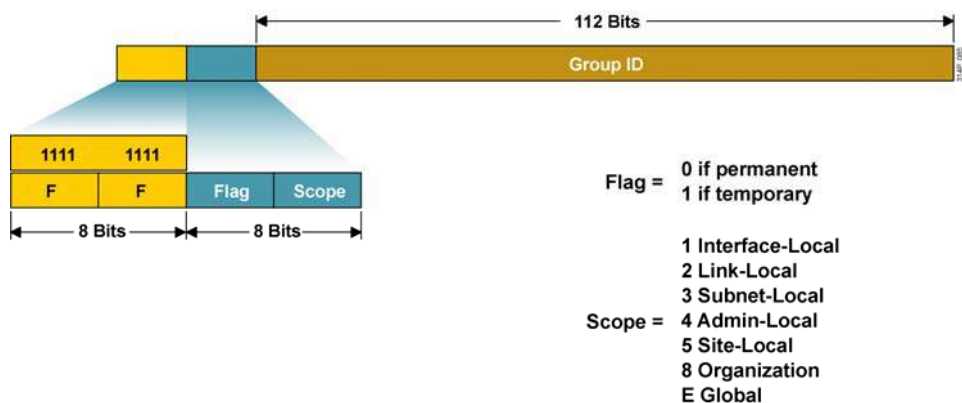







图 5. 链路本地单播地址格式

1.9.5. 组播地址 Multicast

与在 IPv4 中一样，组播地址被分配给一套属于不同节点的接口。发往组播地址的数据包被发送到该地址所确定的所有接口。IPv6 组播地址使用 FF00::/8 前缀，全部 IPv6 地址空间的 1/256



	Meaning		Scope
FF02::1	All nodes		Link-local
FF02::2	All routers		Link-local
FF02::9	All RIP routers		Link-local
FF02::1:FFXX:XXXX	Solicited-node		Link-local
FF05::101	All NTP servers		Site-local

1.9.6. 任意播地址 Anycast

- IPv6 任意播地址是一种新增的地址，这种地址被分配给一组位于不同设备上的接口
- 一个任意播地址标识多个接口
- 发送给任意播地址的数据报文将传输到该地址标识的最近的接口上(取决于使用的路由选择协议)
- 因此，使用相同任意播地址的所有节点应提供相同的服务。
- 任意播地址可用于负载均衡和内容提供服务
- 从组成上看，任意播地址与全局单播地址没什么不同，因为任意播地址来自全局的单播地址空间
- 任意播地址不能用作 IPv6 数据报文的源地址

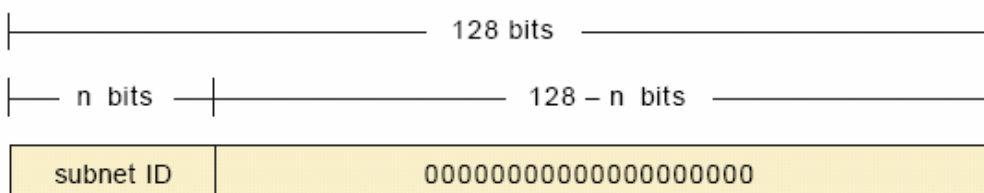


图 6. 任播地址格式

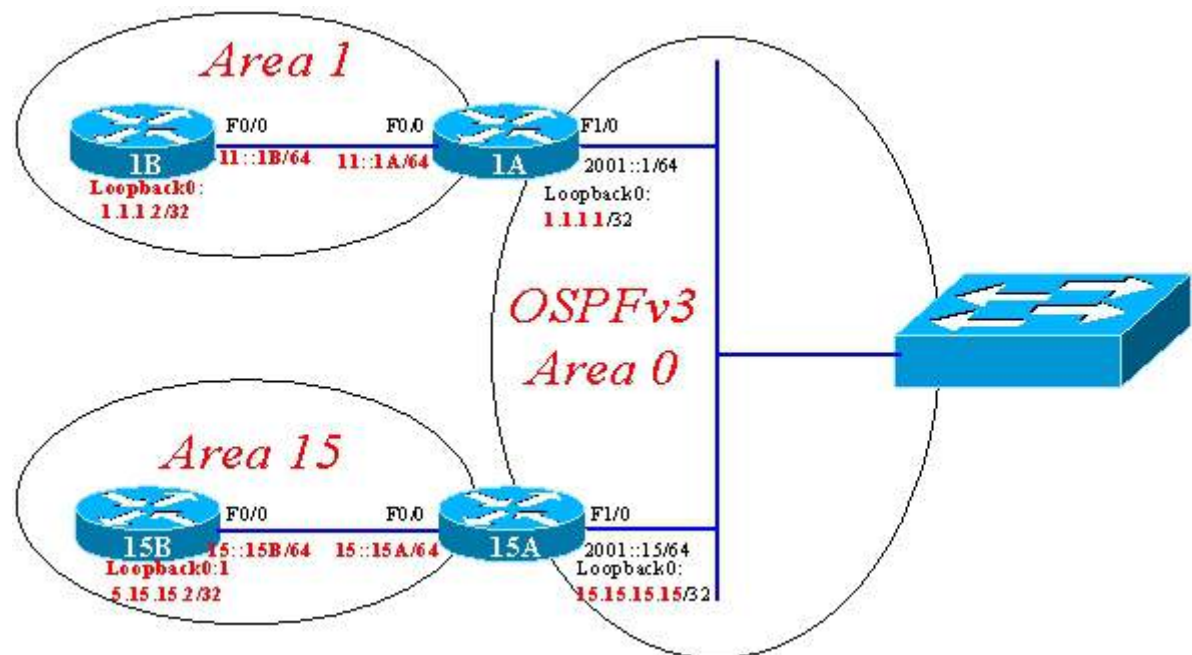
1.9.7. EUI(扩展全局标识)地址格式

EUI-64 格式附加位的以太网接口的 MAC 地址获得。例如，带有以太网接口地址 0003B61A2061

的一个节点，结合由路由器通告提供的网络前缀 2001:0001:1EEF:0000/64，将具有一个如 2001:0001:1EEF:0000:0003:B6FF:FE1A:2061 这样的 IPv6 地址

1.9.8. IPv6 与 OSPFv3 的实验配置

实验目的：各路由器之间启用 OSPFv3 的路由协议，实现各路由上的 IPv6 地址的全局可达性



15A 的 ipv6 基本配置

```
15A(config)# ipv6 unicast-routing
15A(config)# interface F0/0
15A(config-if)# ipv6 address 15::15A/64
15A(config-if)# no shutdown
15A(config-if)# interface F1/0
15A(config-if)# ipv6 address 2001::15/64
15A(config-if)# no shutdown
15A(config-if)# exit
```

15A 的 OSPF 配置

```
15A(config)# ipv6 router ospf 1
15A(config-rtr)# router-id 15.15.15.1
15A(config-rtr)# interface F0/0
15A(config-if)# ipv6 ospf 1 area 15 //将接口发布到区域 15
15A(config-if)# interface F1/0
15A(config-if)# ipv6 ospf 1 area 0 //将接口发布到区域 0
15A(config-if)# end
```

15B 的 ipv6 基本配置

```
15B(config)# ipv6 unicast-routing
15B(config)# interface F0/0
```



```
15B(config-if)# ipv6 address 15::15B/64
```

```
15B(config-if)# no shutdown
```

15B 的 OSPF 配置

```
15B(config)# ipv6 router ospf 1
```

```
15B(config-rtr)# router-id 15.15.15.2
```

```
15B(config)# interface F0/0
```

```
15B(config-if)# ipv6 ospf 1 area 15 //将接口发布到区域 15
```

```
15B(config-if)# end
```

```
15A# show ipv6 ospf neighbor //查 OSPFv3 的邻居信息
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
15.15.15.1	1	FULL/BDR	00:00:36	4	FastEthernet0/0

```
15B# show ipv6 route //查看 IPv6 的路由表
```

```
C 15::/64 [0/0]
```

```
via ::, FastEthernet0/0
```

```
L 15::15B/128 [0/0]
```

```
via ::, FastEthernet0/0
```

```
OI 2001::/64 [110/2]
```

```
via FE80::CE00:13FF:FE5C:0, FastEthernet0/0
```

```
L FE80::/10 [0/0]
```

```
via ::, Null0
```

```
L FF00::/8 [0/0]
```

```
via ::, Null0
```

2. CCNP BCMSN课程

2.1.VLAN(虚拟局域网)

2.1.1. 概念:

- 一个 VLAN 等同于一个子网，一个广播域
- 默认情况下，各交换机的所有接口均属于 VLAN1

- 在二层交换机上，是不能够实现 VLAN 间通信的(说明：需路由支持)
- 建议为每一个 VLAN 分配一个独立的 IP 地址段
- 可以为二层交换机配置一个管理地址
- 交换机会为每一个 VLAN 接口(SVI 接口)分配一个 MAC 地址

2.1.2. VLAN的创建

第 1 种法：全局模式下的创建

```
Switch(config)# vlan 10
Switch(config)# vlan 20
Switch(config)# vlan 30
Switch(config)# vlan 33
```

第 2 种法：特权模式下的创建

```
Switch# vlan database
Switch(vlan)# vlan 10 name ZL-CLASS
Switch(vlan)# vlan 20
Switch(vlan)# vlan 30
Switch(vlan)# vlan 33
Switch# show vlan brief    //查看 vlan 列表
```

2.1.3. VLAN的划分(将相应的接口划分到相应的VLAN)

```
Switch(config)# interface F0/3    (配置单个接口)
Switch(config)# interface range F0/3 , f0/12    (配置两个接口，中间用逗号隔开)
Switch(config)# interface range F0/14 – 22    (配置一组接口，从 F0/14 到 F0/22 范围内的)
Switch(config-if-range)# switchport access vlan 10 //将当前配置的一组接口划分到 vlan10
Switch(config-if-range)# switchport mode access    //设定端口模式为访问链路模式
```

2.1.4. 关于TRUNK链路 (中继链路)

- TRUNK 的特点在于：能够承载传递带有 VLAN 标记的帧
- TRUNK 的链路封装协议有：802.1Q 和 ISL(思科私有协议)
 - a. ISL 链路封装特点在于：在源帧的头部增加一个 26 个字节的新字段
 - b. 802.1Q 链路封装的特点在于：在源帧的内部插入一个 Tag 的标记
- 3、802.1Q 的 Native VLAN：又称本地 VLAN，本地 VLAN 是指不带有 VLAN 标记的帧，可以在 ACCESS 链路或 802.1Q 的 TRUNK 链路中传递。交换机默认的 Native VLAN 为 VLAN 1。

2.1.5. TRUNK链路的配置

说明：建议在各交换机之间的连接链路都配置为 TRUNK 链路

```
Switch(config)# interface f0/24
```

```
Switch(config-if)# switchport trunk encapsulation dot1q    //封装 802.1Q 协议
Switch(config-if)# switchport mode trunk                  //设定链路为 Trunk 模式
Switch(config-if)# switchport trunk allowed vlan all      //默认是允许所有 vlan 通过
查看命令： show interface f0/24 trunk    //查看接口参与 Trunk 的状态
```

```
Switch#show interfaces f0/2 trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/2	on	802.1q	trunking	1

```
Port          Vlans allowed on trunk
```

```
Fa0/2         1-4094
```

```
Port          Vlans allowed and active in management domain
```

```
Fa0/2         1,10,20,30,40,50
```

```
Port          Vlans in spanning tree forwarding state and not pruned
```

```
Fa0/2         1,10,20,30,40,50
```

2.1.6. 关于DTP协议 (动态中继协议)

DTP 的作用：是在两个交换机之间协商接口的连接模式

下图为 DTP 的协商关系

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

2.1.7. VTP 协议(VLAN中继协议)

- 作用：主要是在各交换机之间可以传递和同步整个 VLAN 的信息(说明：Server 端 VLAN 所属的接口是会被传递出去的,只会传递 VLAN 号及 VLAN 名称)。另外在同一 Domain 内才可以实现传递。
- 功能：能够跨越多个交换机，或在交换机之间管理 VLAN 的创建、编辑和删除。
- 工作模式：
 - ✧ Server(服务端模式)：能够创建、编辑、删除 VLAN，且会发送和接收 VLAN 的同步信息，VLAN 信息会被保存在 NVRAM
 - ✧ Transparent(透明模式)：能够创建、编辑、删除本地 VLAN，会转发 VLAN 信息，但不会同步 VLAN 的配置，VLAN 信息会被保存在 NVRAM
 - ✧ Client(客户端模式)：不能够创建、编辑、删除 VLAN，会转发 VLAN 信息，同时，

会接收 VLAN 的同步信息，在特定情况下，也可以发送 VLAN 的同步信息

2.1.8. VTP的实验配置:

说明：在传递 VTP 时，要求各交换机间启用 TRUNK 链路



```
interface f0/23
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)#exit
SW1(config)# vtp domain CCNP //设定 domain 为 CCNP
SW1(config)# vtp mode server //设定模式为: server 端
SW1(config)# vtp password cisco //设定密码为: cisco
SW1(config)# vtp pruning //启用 vtp 修剪
```

```
SW2(config)# interface range f0/23 , f0/20
SW2(config-if)# switchport trunk encapsulation dot1q
SW2(config-if)# switchport mode trunk
SW2(config-if)#exit
SW2(config)# vtp domain CCNP //设定 domain 为 CCNP
SW2(config)# vtp mode transparent //设定模式为: 透明端
SW2(config)# vtp password cisco //设定密码为: cisco
SW2(config)# vtp pruning //启用 vtp 修剪
```

```
SW3(config)# interface f0/20
SW3(config-if)# switchport trunk encapsulation dot1q
SW3(config-if)# switchport mode trunk
SW3(config-if)#exit
SW3(config)# vtp domain CCNP //设定 domain 为 CCNP
SW3(config)# vtp mode client //设定模式为: 客户端
SW3(config)# vtp password cisco //设定密码为: cisco
SW3(config)# vtp pruning //启用 vtp 修剪
```

```
sw3#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 : 0x2F 0x40 0x45 0x46 0x53 0x06 0xA4 0x42

Configuration last modified by 0.0.0.0 at 3-1-93 01:29:04

说明：不管是客户端还是服务端，Configuration Revision 值高的，为发送 VLAN 的同步端

2.2. Spanning tree protocol (STP)生成树协议

2.2.1. 冗余网络中产生的问题

- 重复帧拷贝(收到同一个帧的多个拷贝)
- MAC 地址表不稳定
- 交换环路(说明：交换机转发广播数据帧的原理是除源端口之外的所有端口转发)

2.2.2. 冗余网络的解决方法

启用生成树协议，STP 会自动将形成冗余的多条链路置为阻塞状态，最终形成单条(或逻辑上的单条)线路，从而避免产生环路现象。

2.2.3. BPDU(桥协议数据单元)概念

对于参与 STP 的一个扩展局域网中的所有交换机，它们都通过数据消息的交换来获取网络中其它交换机的信息。这些消息就被称为 BPDU；默认情况下，交换机之间的 BPDU 消息是每隔 2 秒钟发送一次。BPDU 可以完成：

- 根桥和根端口的选举
- 通过阻塞特定的端口来避免环路
- 通告网络的拓扑变更
- 监控生成树的状态

2.2.4. Bridge ID(网桥标识符)概念

Bridge ID 是每一台交换机的唯一名称标识，其主要是由两个部分组成的
MAC 地址 + 优先级(默认为 32768+所属的 VLAN 号)

SW1#show spanning-tree

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0019.e7a0.ce80

说明：Bridge ID 优先级，越低越优先，在进行手动调整时，需按 4096 的倍数递增或递减
如 SW(config)# spanning-tree vlan 1 priority 8192 (4096×2)

2.2.5. 根桥的选举

说明：在同一个广播域内，只允许存在一个根桥，且根桥的所有端口均为指定端口(可接收或发送数据帧)

- 1、选择 Bridge ID 优先级最低的
- 2、选择 Bridge ID MAC 地址最小的

2.2.6. 非根桥中根端口的选举和指定端口的选举

- 1、选择接口 Cost 值最低的
链路速度/COST 值 10GB= 2 1GB= 4 100MB= 19 10MB= 100
修改接口 Cost 值 `SW(config-if)# spanning-tree cost 18`
- 2、选择端口 ID 最小的
- 3、选择 Bridge ID 最小的(顺序为：优先级小→ MAC 小)
- 4、端口优先级最小的 `SW(config-if)# spanning-tree port-priority 112`

2.2.7. 生成树协议的端口状态

- Blocking 阻塞状态 (BLK) 20 秒
在阻塞状态，端口不参与帧的转发，但接收流入进来的 BPDU(桥协议数据单元)
- Listening 监听状态 (LIS) 15 秒
在监听状态，可以进行根桥、根端口、指定端口和非指定端口的选举，但不参与数据帧的转发
- Learning 学习状态 (LRN) 15 秒
学习流入进来的 MAC 地址，准备参与数据帧的转发
- Forwarding 转发状态 (FWD)
接口参与数据帧的转发

2.2.8. 常用增强型生成树协议：

PVST(每一个 vlan 一个生成树协议)

PVST+ 增强型的 PVST

RSTP 快速生成树协议

`SW(config)# spanning-tree mode rapid-pvst`

2.2.9. 高级的STP特性

- PortFast 端口(快速端口)

PortFast 的目的是尽量缩短接入端口等待 STP 的收敛时间。启用 PortFast 的优势在于能够免除不必要的 STP 环路计算，让这些不可能存在桥接环路的端口直接置为快速转发。通常该类接口特性应用于连接：PC 终端、服务器、路由器等

`SW(config)# interface range f0/1 -22`

`SW(config-if-range)# spanning-tree portfast` //接口模式启用 portfast 特性

SW(config)# spanning-tree portfast default //全局模式启用 portfast 特性

注意：如果启用 PortFast 特性的端口接收到交换机发过来的 BPDU 消息，BPDU 防护使得端口进入 err-disable 状态，err-disable 状态等效于禁用状态，如果出现这样的状态，可以进入接口先手动 shutdown，再手动 no shutdown 即可恢复。

➤ UplinkFast 上行快速链路

UplinkFast 是用在访问层交换机上的，而且是用在有阻塞端口的交换机上。当根端口出现故障时，马上启用阻塞端口保持通信。这样收敛的时间会得到很快，不用重新进行 STP 运算，将直接从 Blocking 过渡到 Forwarding 状态。

注意：当启用 UplinkFast 特性后，它将影响到交换机上所有的 VLAN。交换机不支持以 VLAN 为基础来配置 UplinkFast 的特性

SW(config)# spanning-tree uplinkfast //全局模式启用 uplinkfast 特性

➤ BackboneFast 快速骨干链路

BackboneFast 是用在分布层交换机上。而且要求所有分布层交换机都得启用 BackboneFast 的特性，该特性的目的就是能够让分布层交换机在与根桥断开时，能够快速收敛。当一台交换机的根端口出现故障时，失去了和根桥的连接，它将向它的其他端口：阻塞端口(如果有的话)发送下级 BPDU。收到下级 BPDU 的交换机有 3 种情况：

1、如果收到下级 BPDU 的端口是阻塞端口，那么阻塞端口和根端口都作为候选端口（用来到达根桥用的）

2、如果收到下级 BPDU 的端口是根端口，那么阻塞端口被作为候选端口，因为只能通过它到达根桥了

3、如果收到下级 BPDU 的端口是根端口，并且这个交换机上没有阻塞端口，那么证明这台交换机失去了到根桥的连接，需要从新进行 STP 运算

交换机中只要有一台处于第三种状态，就要从新进行 STP 运算。除此之外，backbone 它的作用就是可以在不是相邻链的网络故障中，缩减网络收敛的时间，通俗点说就是省去了 20 秒的最大老化时间。

SW(config)# spanning-tree backbonefast //全局模式启用 backbonefast 特性

2.2.10. 提高生成树的弹性机制

STP 不提供检测机制和平衡机制来确保多层交换网络的高可用性，可使用 BPDU 防护、和根防护来提高 STP 的弹性

- BPDU 防护：能够防止交换机设备意外地连接到启用 PortFast 特性的端口，如果将交换机连接到启用 PortFast 特性的端口，那么就可能会导致 2 层环路。

SW(config)# spanning-tree portfast bpduguard //全局模式启用 BPDU 防护

- 根防护：能够强制让接口成为指定端口，进而能够防止周围的交换机成为根交换机。

2.2.11. MSTP 多生成树协议

- 将多个 VLAN 划分到属于 MSTP 的一个实例(Instance)中

- 交换机只需要维护一个实例即可，相当于维护一个生成树协议

SW1(config)#spanning-tree mode mst

SW1(config)#spanning-tree mst configuration

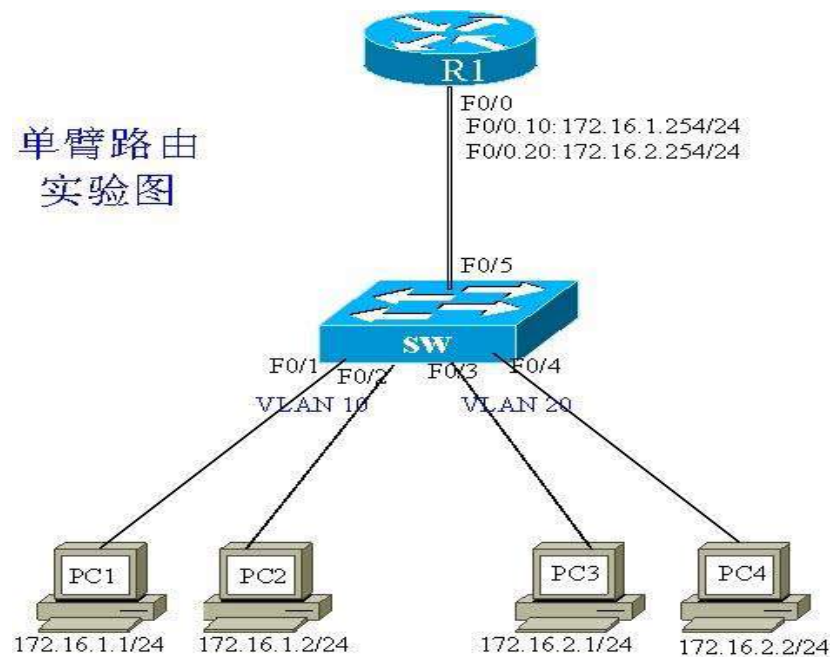
SW1(config-mst)#instance 10 vlan 1-30

```
SW1(config-mst)#instance 20 vlan 31-50
```

```
SW1(config-mst)#instance 30 vlan 51-10
```

2.3. 2 层/3 层 VLAN 间路由

2.3.1. 单臂路由(2 层交换机+ 路由器)实现VLAN间通信



```
SW(config)# vlan 10
```

```
SW(config-vlan)# vlan 20
```

```
SW(config-vlan)# interface range f0/1 – f0/2
```

```
SW(config-if-range)# switchport access vlan 10
```

```
SW(config-if-range)# switchport mode access
```

```
SW(config-if-range)# interface range f0/3 – f0/4
```

```
SW(config-if-range)# switchport access vlan 20
```

```
SW(config-if-range)# switchport mode access
```

```
SW(config-if-range)# interface f0/5
```

```
SW(config-if)# switchport trunk encapsulation dot1q
```

```
SW(config-if)# switchport mode trunk
```

```
SW(config-if)# end
```

```
R1(config)# interface F0/0
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# interface F0/0.10
```

```
R1(config-subif)# encapsulation dot1q 10
```

```
R1(config-subif)# ip address 172.16.1.254 255.255.255.0
```

```
R1(config-subif)# interface F0/0.20
```

```
R1(config-subif)# encapsulation dot1q 20
```

```
R1(config-subif)# ip address 172.16.2.254 255.255.255.0
```

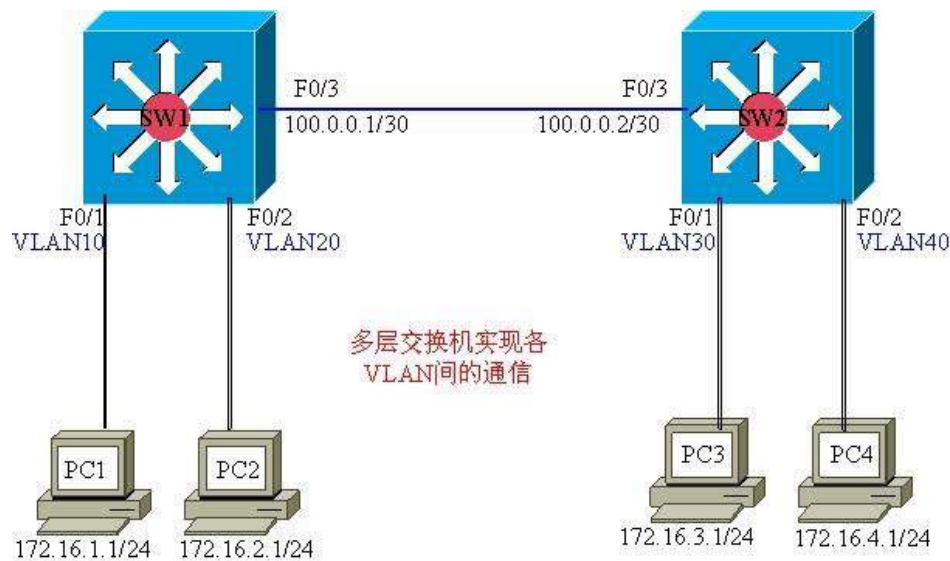
```
R1(config-subif)# end
```


说明：PC 机可以使用路由器来进行模拟 如：
Router(config)# no ip routing //关闭路由功能
Router(config)# ip default-gateway 172.16.1.254 //设定网关

验证方法：在 PC1 上能够 ping 通 PC4 即可
实验完成

2.3.2. 多层交换机实现VLAN间路由实验

实验目的：在多层交换机之间实现各 VLAN 间的通信



```
SW1(config)# vlan 10
SW1(config-vlan)# vlan 20
SW1(config)# interface F0/1
SW1(config-if)# switchport access vlan 10
SW1(config-if)# switchport mode access
SW1(config-if)# spanning-tree portfast
SW1(config-if)# interface F0/2
SW1(config-if)# switchport access vlan 20
SW1(config-if)# switchport mode access
SW1(config-if)# spanning-tree portfast
SW1(config-if)# interface vlan 10
SW1(config-if)# ip address 172.16.1.254 255.255.255.0
SW1(config-if)# interface vlan 20
SW1(config-if)# ip address 172.16.2.254 255.255.255.0
SW1(config-if)# interface F0/3
SW1(config-if)# no switchport
SW1(config-if)# ip address 100.0.0.1 255.255.255.252
SW1(config-if)# exit
SW1(config)# ip routing
SW1(config)# ip route 172.16.3.0 255.255.255.0 100.0.0.2
```

```
SW1(config)# ip route 172.16.4.0 255.255.255.0 100.0.0.2
```

```
SW2(config)# vlan 30
SW2(config-vlan)# vlan 40
SW2(config)# interface F0/1
SW2(config-if)# switchport access vlan 30
SW2(config-if)# switchport mode access
SW2(config-if)# spanning-tree portfast
SW2(config-if)# interface F0/2
SW2(config-if)# switchport access vlan 40
SW2(config-if)# switchport mode access
SW2(config-if)# spanning-tree portfast
SW2(config-if)# interface vlan 30
SW2(config-if)# ip address 172.16.3.254 255.255.255.0
SW2(config-if)# interface vlan 40
SW2(config-if)# ip address 172.16.4.254 255.255.255.0
SW2(config-if)# interface F0/3
SW2(config-if)# no switchport
SW2(config-if)# ip address 100.0.0.2 255.255.255.252
SW2(config-if)# exit
SW2(config)# ip routing
SW2(config)# ip route 172.16.1.0 255.255.255.0 100.0.0.1
SW2(config)# ip route 172.16.2.0 255.255.255.0 100.0.0.1
```

验证方法：各 PC 机之间能够相互 ping 通，即实验完成

2.4.HSRP 热备份冗余路由协议

2.4.1. HSRP的概念

HSRP：热备份路由器协议（HSRP：Hot Standby Router Protocol）

热备份路由器协议（HSRP）的设计目标是支持特定情况下 IP 流量失败转移不会引起混乱、并允许主机使用单路由器，以及即使在实际第一跳路由器使用失败的情形下仍能维护路由器间的连通性。换句话说，当源主机不能动态知道第一跳路由器的 IP 地址时，HSRP 协议能够保护第一跳路由器不出故障。该协议中含有多种路由器，对应一个虚拟路由器。HSRP 协议只支持一个路由器代表虚拟路由器实现数据包转发过程。终端主机将它们各自的数据包转发到该虚拟路由器上。

负责转发数据包的路由器称之为主动路由器（Active Router）。一旦主动路由器出现故障，HSRP 将激活备份路由器（Standby Routers）取代主动路由器。HSRP 协议提供了一种决定使用主动路由器还是备份路由器的机制，并指定一个虚拟的 IP 地址作为网络系统的缺省网关地址。如果主动路由器出现故障，备份路由器（Standby Routers）承接主动路由器的

2.4.2. HSRP技术在网络中的应用

一、HSRP 协议概述

实现 HSRP 的条件是系统中有多台路由器，它们组成一个“热备份组”，这个组形成一个虚拟路由器。在任一时刻，一个组内只有一个路由器是活动的，并由它来转发数据包，如果活动路由器发生了故障，将选择一个备份路由器来替代活动路由器，但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器切换的问题。

为了减少网络的数据流量，在设置完活动路由器和备份路由器之后，只有活动路由器和备份路由器定时发送 HSRP 报文。如果活动路由器失效，备份路由器将接管成为活动路由器。如果备份路由器失效或者变成了活动路由器，将有另外的路由器被选为备份路由器。

二、HSRP 的工作原理

HSRP 协议利用一个优先级方案来决定哪个配置了 HSRP 协议的路由器成为默认的主动路由器。如果一个路由器的优先级设置的比所有其他路由器的优先级高，则该路由器成为主动路由器。路由器的缺省优先级是 100，所以如果只设置一个路由器的优先级高于 100，则该路由器将成为主动路由器。

通过在设置了 HSRP 协议的路由器之间广播 HSRP 优先级，HSRP 协议选出当前的主动路由器。当在预先设定的一段时间内主动路由器不能发送 hello 消息时，优先级最高的备用路由器变为主动路由器。路由器之间的包传输对网络上的所有主机来说都是透明的。

配置了 HSRP 协议的路由器交换以下三种多点广播消息：

Hello——hello 消息通知其他路由器发送路由器的 HSRP 优先级和状态信息，HSRP 路由器默认为每 3 秒钟发送一个 hello 消息；

Coup——当一个备用路由器变为一个主动路由器时发送一个 coup 消息；

Resign——当主动路由器要宕机或者当有优先级更高的路由器发送 hello 消息时，主动路由器发送一个 resign 消息。在任一时刻，配置了 HSRP 协议的路由器都将处于以下六种状态之一：

Initial——HSRP 启动时的状态，HSRP 还没有运行，一般是在改变配置或端口刚刚启动时进入该状态。

learn——路由器已经得到了虚拟 IP 地址，但是它既不是活动路由器也不是等待路由器。它一直监听从活动路由器和等待路由器发来的 HELLO 报文。

Listen——路由器正在监听 hello 消息。

Speak——在该状态下，路由器定期发送 HELLO 报文，并且积极参加活动路由器或等待路由器的竞选。

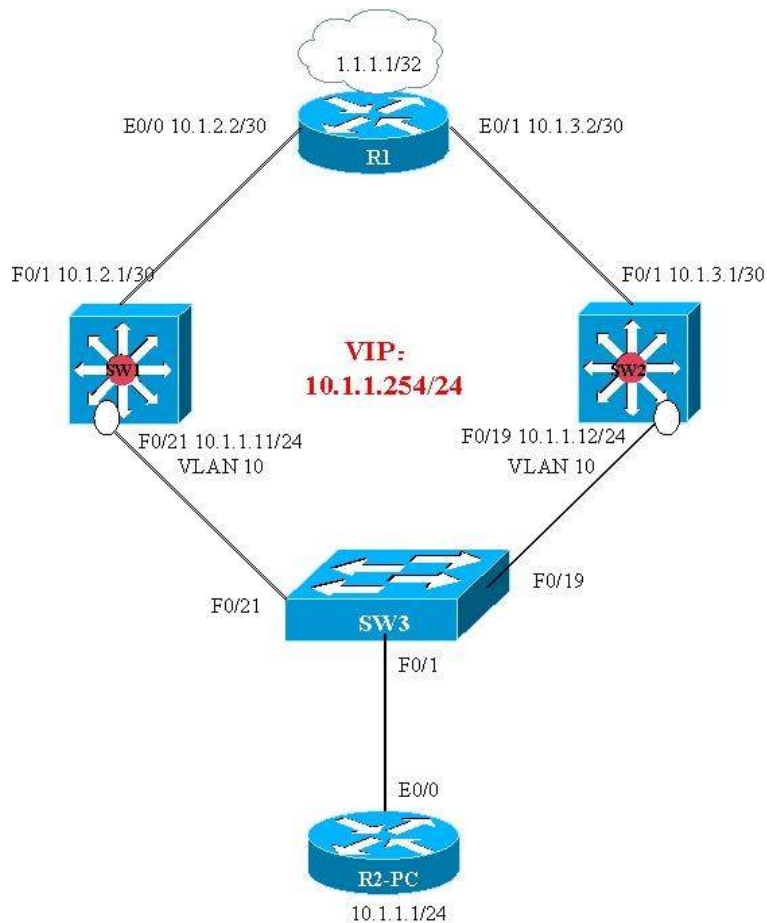
Standby——当主动路由器失效时路由器准备接管包传输功能。

Active——路由器执行包传输功能。

2.4.3. HSRP的实验

实验目的：R2-PC 的机器可以 ping 通远端网络中的 IP: 1.1.1.1 地址，当 SW1 或 SW2 中某一条上行链路或下行链路出现故障时，能够自动切换，并能够持续跟 1.1.1.1 这个远端的主机实施通信。

实验拓扑图如下：



```
R2-PC(config)# interface e0/0
R2-PC(config-if)# ip address 10.1.1.1 255.255.255.0
R2-PC(config-if)# exit
R2-PC(config)# no ip routing
R2-PC(config)# ip default-gateway 10.1.1.254
```

```
R1(config)#router eigrp 100
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.0.0
R1(config-router)# network 1.0.0.0
R1(config-router)#
```

```
SW1(config)#ip routing
SW1(config)#router eigrp 100
SW1(config-router)#no auto-summary
SW1(config-router)#network 10.0.0.0
SW1(config-router)#exit
SW1(config)#interface vlan 10
SW1(config-if)# ip address 10.1.1.11 255.255.255.0
SW1(config-if)# standby 7 ip 10.1.1.254 //配置虚拟网关地址
SW1(config-if)# standby 7 priority 200 //设定主网关的高优先级
SW1(config-if)# standby 7 preempt //启用抢占功能
SW1(config-if)# standby 7 track f0/1 80 //调用跟踪事件,若发现上行链路 down,则降低 80,
```

200-80=120

SW1#show standby

```
SW2(config)#ip routing
SW2(config)#router eigrp 100
SW2(config-router)#no auto-summary
SW2(config-router)#network 10.0.0.0
SW2(config-router)#exit
SW2(config)#interface vlan 10
SW2(config-if)# ip address 10.1.1.12 255.255.255.0
SW2(config-if)# standby 7 ip 10.1.1.254    //配置虚拟网关地址
SW2(config-if)# standby 7 priority 150      //设定主网关的高优先级
SW2(config-if)# standby 7 preempt          //启用抢占功能
SW2#show standby
```

2.5.VRRP 虚拟路由器冗余协议

2.5.1. VRRP 虚拟路由器冗余协议

VRRP 协议的工作原理跟 HSRP 基本一样

VRRP 协议是一个公用的标准协议，各厂商的设备都支持，原理与 HSRP 几乎是一样
实验拓扑图使用 HSRP 的实验拓扑，实验目的跟 HSRP 一样
使用 HSRP 的实验图完成 VRRP 实验

```
R2-PC(config)# interface e0/0
R2-PC(config-if)# ip address 10.1.1.1 255.255.255.0
R2-PC(config-if)# exit
R2-PC(config)# no ip routing
R2-PC(config)# ip default-gateway 10.1.1.254
```

```
R1(config)#router eigrp 100
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.0.0
R1(config-router)# network 1.0.0.0
R1(config-router)#
```

```
SW1(config)#ip routing
SW1(config)#router eigrp 100
SW1(config-router)#no auto-summary
SW1(config-router)#network 10.0.0.0
SW1(config-router)#exit
SW1(config)#interface vlan 10
SW1(config-if)# ip address 10.1.1.11 255.255.255.0
SW1(config-if)# vrrp 7 ip 10.1.1.254    //配置虚拟网关地址
SW1(config-if)# vrrp 7 priority 200      //设定主网关的高优先级
SW1(config-if)# vrrp 7 preempt          //启用抢占功能
```

```
SW1(config)# track 10 interface f0/1 line-protocol //创建事件号, 全局模式配置
SW1(config-if)# vrrp 7 track 10 decrement 80 //调用跟踪事件,若发现上行链路 down,则降低 80,
200-80=120
SW1#show vrrp
```

```
SW2(config)#ip routing
SW2(config)#router eigrp 100
SW2(config-router)#no auto-summary
SW2(config-router)#network 10.0.0.0
SW2(config-router)#exit
SW2(config)#interface vlan 10
SW2(config-if)# ip address 10.1.1.12 255.255.255.0
SW2(config-if)# vrrp 7 ip 10.1.1.254 //配置虚拟网关地址
SW2config-if# vrrp 7 priority 150 //设定主网关的高优先级
SW2(config-if)# vrrp 7 preempt //启用抢占功能
SW2#show vrrp
```

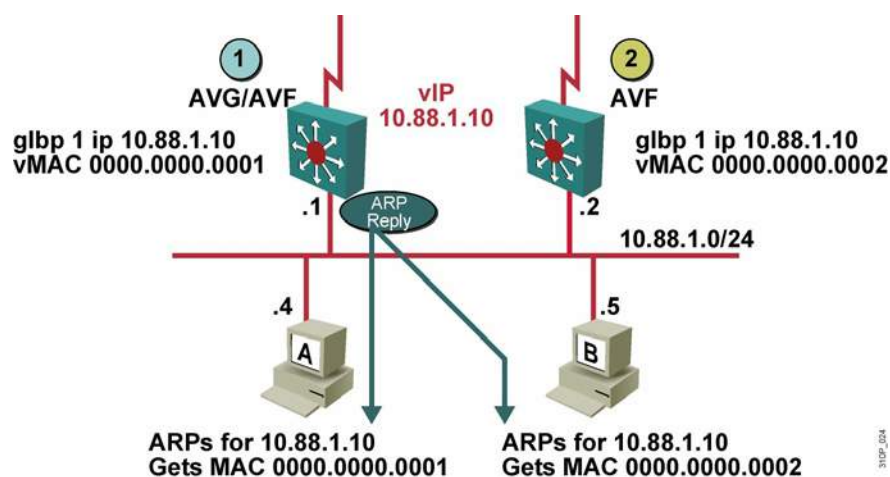
2.6. GLBP 网关负载均衡协议

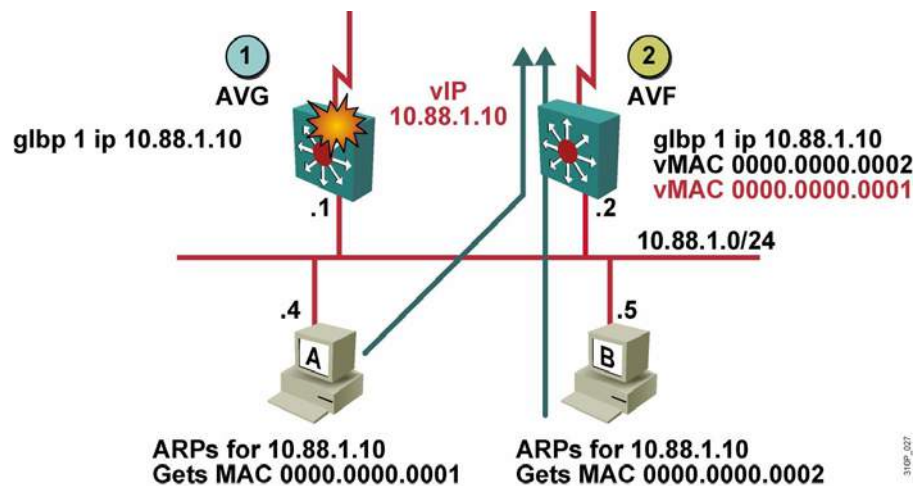
2.6.1. GLBP 网关负载均衡协议

GLBP 是思科的私有协议，在一般高端设备才会支持全称 Gateway Load Balancing Protocol

- 和 HSRP、VRRP 不同的是，GLBP 不仅提供冗余网关，还在各网关之间提供负载均衡，而 HSRP、VRRP 都必须选定一个活动路由器，而备用路由器则处于闲置状态。
- 和 HSRP 不同的是，GLBP 可以绑定多个 MAC 地址到虚拟 IP，从而允许客户端选择不同的路由器作为其默认网关，而网关地址仍使用相同的虚拟 IP，从而实现一定的冗余。

1、一个虚拟 IP 地址允许有多个 MAC 地址





```
SW1(config)#ip routing
SW1(config)#router eigrp 100
SW1(config-router)#no auto-summary
SW1(config-router)#network 10.0.0.0
SW1(config-router)#exit
SW1(config)#interface vlan 10
SW1(config-if)# ip address 10.1.1.11 255.255.255.0
SW1(config-if)# glbp 7 ip 10.1.1.254 //配置虚拟网关地址
SW1(config-if)# glbp 7 priority 200 //设定主网关的高优先级
SW1(config-if)# glbp 7 preempt //启用抢占功能
SW1(config)# track 10 interface f0/1 line-protocol //创建事件号，全局模式配置
SW1(config-if)# glbp 7 weighting track 10 decrement 80 //调用跟踪事件,若发现上行链路 down,则降低 80, 200-80=120
SW1#show glbp
```

```
SW2(config)#ip routing
SW2(config)#router eigrp 100
SW2(config-router)#no auto-summary
SW2(config-router)#network 10.0.0.0
SW2(config-router)#exit
SW2(config)#interface vlan 10
SW2(config-if)# ip address 10.1.1.12 255.255.255.0
SW2(config-if)# glbp 7 ip 10.1.1.254 //配置虚拟网关地址
SW2(config-if)# glbp 7 priority 150 //设定主网关的高优先级
SW2(config-if)# glbp 7 preempt //启用抢占功能
SW2#show glbp
```

2.7.WLAN(无线局域网)

2.7.1. WLAN的无线技术标准

- 协议标准：IEEE 802.11a, 802.11b, 802.11g
- 传输距离：中等距离，几十米至几百米范围
- 传输速率：1-54M
- 应用范围：企业或家庭

2.7.2. WLAN的基本概念

- WLAN 是一个共享式的网络
- AP(访问点)设备相当于以太网中的 HUB(集线器)
- 数据的传输是基于无线电波
- 双向的无线电通信采用的是半双工机制
- 要求在同一个无线电波频率下发送或接收数据

2.7.3. SSID(服务集标识符)

SSID 是用来作为一个无线网络设备的标识，这个标识通常是独一无二，需要手动设置和配置。一个无线网卡同时只能够连接到一个 AP 设备上。

2.7.4. 无线应用技术标准

无线标准为：802.11

- 802.11b : 工作在 2.4GHZ 频段；采用 DSSS(直接序列的展频)技术；提供了 4 种传输速率：1M 、 2M、 5.5M、 11M，工作通道为： 1 、 6 、 11
- 802.11a : 工作在 5GHZ 频段；采用 OFDM(正交频分复用)技术；提供了 8 种传输速率：6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M，工作通道为： 36 、 44 、 52 、 60
- 802.11g : 工作在 2.4GHZ 频段；采用 DSSS 和 OFDM 两项技术，同时可以兼容 802.11b 的标准，提供了多种接入速率，工作通道为： 1、 6、 11

2.7.5. 无线的安全

WEP 是一种在接入点和客户端之间以“RC4”方式对分组信息进行加密的技术，密码很容易被破解。WEP 使用的加密密钥包括收发双方预先确定的 40 位（或者 104 位）通用密钥，和发送方为每个分组信息所确定的 24 位、被称为 IV 密钥的加密密钥。但是，为了将 IV 密钥告诉给通信对象，IV 密钥不经加密就直接嵌入到分组信息中被发送出去。如果通过无线窃听，收集到包含特定 IV 密钥的分组信息并对其进行解析，那么就连秘密的通用密钥都可能被计算出来。

WPA 是继承了 WEP 基本原理而又解决了 WEP 缺点的一种新技术。由于加强了生成加密密钥的算法，因此即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。

2.7.6. 使用WEB方式配置无线AP设备

设备型号： AIR-AP1232AG

一般情况下，第一次配置 AP 时，可以使用 Console 口进行连接，登陆进去后，先配置管理 IP 地址：

```
AP(config)# interface BVI1
```

```
AP(config-if)# ip address 192.168.2.2 255.255.255.0
```

```
AP(config-if)# no shutdown
```

```
AP(config-if)# exit
```

```
AP(config)# ip http server //开启支持 Web 的管理功能
```

```
AP(config)# username zltrain privilege 15 password cisco //设定管理员帐户名和密码
```

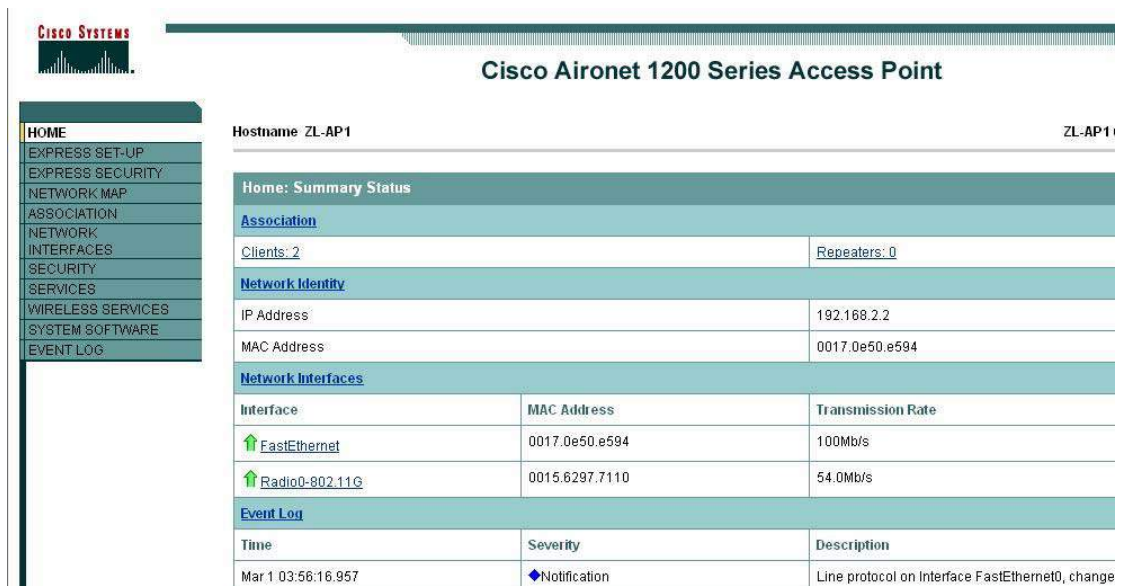
说明：默认无线 AP 的默认 enable 密码为：Cisco //注意，C 为大写，后面的字母为小写
打开IE浏览器，输入 <http://192.168.2.2> 会出现下列登陆框，要求输入用户名和密码



The image shows a Windows-style dialog box titled "连接到 192.168.2.2". It contains a login form with the following fields and controls:

- Username (U): A text box containing "zltrain".
- Password (P): A text box with masked characters "*****".
- Remember my password (R): An unchecked checkbox.
- Buttons: "确定" (OK) and "取消" (Cancel).

完成后，即可正式进入 AP 的管理界面：



The image displays the web management interface for a Cisco Aironet 1200 Series Access Point. The interface includes a sidebar menu, a header with the Cisco logo and device name, and a main content area showing configuration details.

Header: Cisco Systems logo, Cisco Aironet 1200 Series Access Point, Hostname: ZL-AP1, ZL-AP1

Sidebar Menu: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, EVENT LOG.

Main Content Area:

- Home: Summary Status**
- Association**
- Network Identity**
- Network Interfaces**
- Event Log**

Interface	MAC Address	Transmission Rate
FastEthernet	0017.0e50.e594	100Mb/s
Radio0-802.11G	0015.6297.7110	54.0Mb/s

Time	Severity	Description
Mar 1 03:56:16.957	Notification	Line protocol on Interface FastEthernet0, change

相关的无线参数配置都可以直接点击左边的工具条进行参数设置

2.8. 以太网通道(链路汇聚)

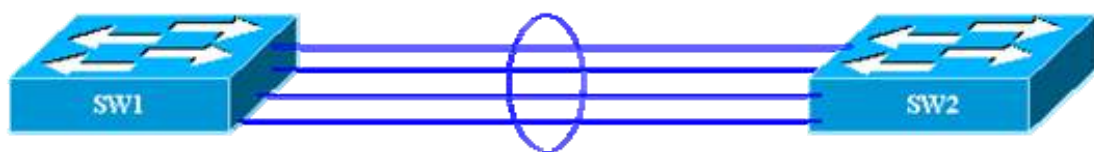
2.8.1. 特点:

- 将多个(最多 8 个)相似的物理端口划分到一个逻辑的端口中
- 在数据的传输中, 能够做到负载均衡
- 多条线路的捆绑, 不会产生 STP 的环路, 有很好的链路冗余

2.8.2. 链路汇聚协议

- 1、PAgP (端口汇聚协议), 属 Cisco 私有协议
 - On 这种模式会强制端口成为 EtherChannel
 - Off 在任何情况下, 接口都不参与 EtherChannel
 - Auto 这种模式会使得接口进入被动协商进程中
 - Desirable 这种模式利用 PAgP 进入主动协商状态 (配置时的推荐模式)
- 2、LACP (链路汇聚控制协议), 802.3ad 标准协议
 - On 强制端口成为 EtherChannel
 - Off 接口不参与 EtherChannel
 - Passive 使得接口进入被动协商进程中
 - Active 进入主动协商状态 (配置时的推荐模式)

2.8.3. 二层Etherchannel实验配置



```
SW1(config)# interface range f0/23 , f0/24
SW1(config-if-range)# channel-group 3 mode desirable
SW1(config-if-range)# exit
SW1(config)# interface port-channel 3    //简写 int po3
SW1(config-if)# switchport trunk encapsulation dot1q
SW1(config-if)# switchport mode trunk
SW1(config-if)# end
```

```
SW2(config)# interface range f0/23 , f0/24
SW2(config-if-range)# channel-group 3 mode desirable
SW2(config-if-range)# exit
SW2(config)# interface port-channel 3    //简写 int po3
SW2(config-if)# switchport trunk encapsulation dot1q
```

```
SW2(config-if)# switchport mode trunk
SW2(config-if)# end
```

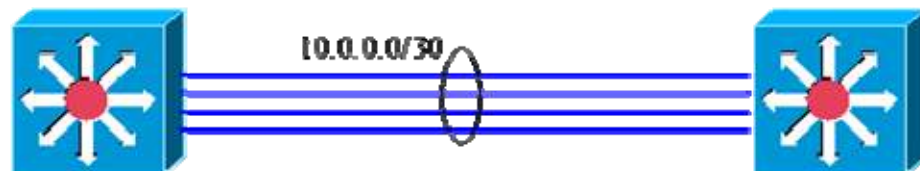
```
SW1# show spanning-tree //查看 STP 的端口状态
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po3	Root FWD	12	128.72	P2p	

```
SW1#show etherchannel summary
```

Group	Port-channel	Protocol	Ports
3	Po3(SU)	PAgP	Fa0/23(P) Fa0/24(P)

2.8.4. 三层Etherchannel实验配置



```
SW1(config)# interface range f0/23, f0/24
SW1(config-if-range)# no switchport //将端口置为 3 层路由口
SW1(config-if-range)# channel-group 11 mode on
SW1(config-if-range)# exit
SW1(config)# interface port-channel 11 //简写 int po11
SW1(config-if)# ip address 10.0.0.1 255.255.255.252
SW1(config-if)# end
```

```
SW2(config)# interface range f0/23, f0/24
SW2(config-if-range)# no switchport
SW2(config-if-range)# channel-group 11 mode on
SW2(config-if-range)# exit
SW2(config)# interface port-channel 11 //简写 int po11
SW2(config-if)# ip address 10.0.0.2 255.255.255.252
SW2(config-if)# end
```

```
SW1#show etherchannel summary
```

Group	Port-channel	Protocol	Ports
11	Po11(RU)	-	Fa0/23(P) Fa0/24(P)

2.9. 交换机的端口安全(Port Security)

2.9.1. 在交换机的接口下配置端口安全

```
SW1(config)# interface FastEthernet0/1
SW1(config-if)# switchport mode access    //设为访问模式，不允许为动态协商
SW1(config-if)# switchport port-security   //在该接口下启用端口安全
SW1(config-if)# switchport port-security violation restrict    //shutdown/ protect/ restrict
SW1(config-if)# switchport port-security mac-address 00b0.6451.c920    //允许通过的 MAC
SW1(config-if)# spanning-tree portfast    //连接 PC 的端口可以设定为 portfast
SW1(config-if)# end
SW1# show port-security
SW1#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	1	1	0	Protect

```
SW1# show port-security interface F0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Protect
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 00b0.6451.c920:1
Security Violation Count : 0
```

2.9.2. 在交换机上实施IP与MAC的双向绑定

说明：不能够在二层交换上做基于 IP 的双向绑定，但可在三层交换机上完成

```
SW1(config)# interface FastEthernet0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security violation restrict    //shutdown protect restrict
SW1(config-if)# switchport port-security mac-address 00b0.6451.c920
SW1(config-if)# spanning-tree portfast
SW1(config-if)# ip access-group 11 in    //调用 ACL
SW1(config-if)# exit
SW1(config)# access-list 11 permit 192.168.2.69
```

2.10. pVLAN(私有VLAN)

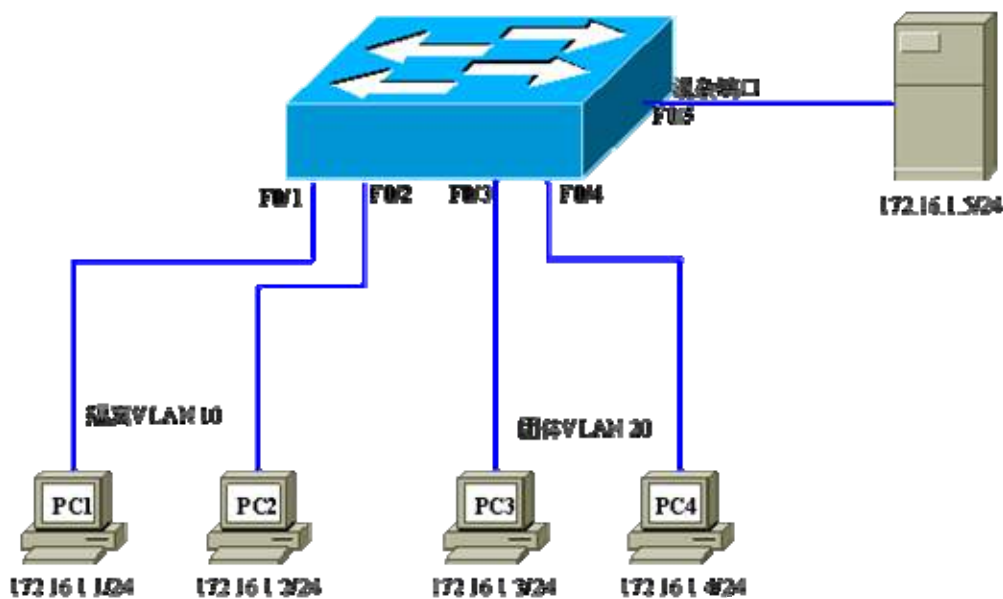
2.10.1. 概念术语

- Primary VLAN 主 VLAN
- Secondary VLAN 辅助 VLAN
 - Isolated vlan 隔离 VLAN
 - Community vlan 团体 VLAN
- Promiscuous port 混杂端口

解释:

- Primary VLAN: 是一个全局 VLAN 的标识
- Isolated VLAN: 同属一个隔离 VLAN 间的用户是不能够互相访问的,但是可以跟主 VLAN 和混杂端口通信
- Community VLAN: 同属同一个团体 VLAN 内的用户,是能够直接互相访问的,且可以跟主 VLAN 和混杂端口通信
- Promiscuous port: 连接计费服务器、网关或路由器等,可以跟所有的其它端口通信

2.10.2. 实验拓扑及配置



配置方法(参考):

//划分主 VLAN

```
Switch(config)# vtp mode transparent //VTP 设为透明模式
```

```
Switch(config)#vlan 800
```

```
Switch(config-vlan)#private-vlan primary
```

//划分团体 VLAN

```
Switch(config)#vlan 511
```

```
Switch(config-vlan)#private-vlan community
```

//划分隔离 VLAN

```
Switch(config)#vlan 522
```

```
Switch(config-vlan)#private-vlan isolated
```

//设定某一物理端口为混杂端口 F0/5

```
Switch(config)#interface F0/5
```

```
Switch(config-if)# switchport mode private-vlan promiscuous
```

```
Switch(config-if)# switchport private-vlan mapping 800 add 511,522
```

//将团体 VLAN 和隔离 VLAN 与主 VLAN 关联

```
Switch(config)#vlan 800
```

```
Switch(config-vlan)#private-vlan association 511,522
```

//将团体 VLAN 511 关联到 F0/10 和 F0/11 接口上，并能够与主 VLAN 800 进行通信

```
Switch(config)#interface range F0/10 , f0/11
```

```
Switch(config-if-range)#switchport mode private-vlan host
```

```
Switch(config-if-range)#switchport private-vlan host-association 800 511
```

//将隔离 VLAN 522 关联到 F0/20 和 F0/21 接口上，并能够与主 VLAN 800 进行通信

```
Switch(config)#interface range F0/20 , f0/21
```

```
Switch(config-if-range)#switchport mode private-vlan host
```

```
Switch(config-if-range)#switchport private-vlan host-association 800 522
```

//将其它各个辅助 VLAN 映射到主 VLAN 中，以实现跟主 VLAN 进行直接通信

```
Switch(config)#interface vlan 800
```

```
Switch(config-if)#private-vlan mapping 511,522
```

pVLAN 实验的完整配置如下：（交换机配置）

```
SW(config)# vlan 10
```

```
SW(config-vlan)# private-vlan isolated
```

```
SW(config)# vlan 20
```

```
SW(config-vlan)# private-vlan community
```

```
SW(config)# vlan 800
```

```
SW(config-vlan)# private-vlan primary
```

```
SW(config-vlan)#private-vlan association 10,20
```

```
SW(config)# interface FastEthernet0/1
```

```
SW(config-if)# switchport private-vlan host-association 800 10
```

```
SW(config-if)# switchport mode private-vlan host
```

```
SW(config-if)# spanning-tree portfast
```

```
SW(config)# interface FastEthernet0/2
```

```
SW(config-if)# switchport private-vlan host-association 800 10
```

```
SW(config-if)# switchport mode private-vlan host
```

```
SW(config-if)# spanning-tree portfast
```

```
SW(config)# interface FastEthernet0/3
```

```
SW(config-if)# switchport private-vlan host-association 800 20
```

```
SW(config-if)# switchport mode private-vlan host
```

```

SW(config-if)# spanning-tree portfast
SW(config)# interface FastEthernet0/4
SW(config-if)# switchport private-vlan host-association 800 20
SW(config-if)# switchport mode private-vlan host
SW(config-if)# spanning-tree portfast
SW(config)# interface FastEthernet0/5
SW(config-if)# switchport private-vlan mapping 800 10,20
SW(config-if)# switchport mode private-vlan promiscuous
SW(config-if)# spanning-tree portfast
SW(config)# interface Vlan800
SW(config-if)# private-vlan mapping 10,20
SW(config-if)# end

```

测试结果：隔离 VLAN 10 之间不能够通信，但可以跟 SERVER 端口通信

团体 VLAN 20 不能跟隔离 VLAN 通信，可以跟自己 VLAN 内的用户通信，同时也可以跟 SERVER 端口通信

混杂端口可以跟所有的用户进行通信

2.11. DHCP Snooping/ IPSPG /DAI

2.11.1. 关于DHCP的欺骗攻击

- 一个 DHCP 的攻击者，同样可以在一个 VLAN 中提供 SERVER 服务
- DHCP 攻击者同样也会应答 DHCP 客户端的发送请求信息
- 攻击者会分配 IP 地址等信息和默认网关给 DHCP 客户端

说明：在一个 VLAN 中存在多个 DHCP 服务器可能会造成地址分配冲突问题

2.11.2. 解决DHCP的欺骗攻击(DHCP Snooping DHCP监听)

- DHCP Snooping 允许配置 trusted(信任)端口和 untrusted(非信任)端口
- Untrusted 端口不能够处理 DHCP 的应答消息
- DHCP Snooping 被配置在 DHCP Server 的上行链路的(接入层)交换机上

2.11.3. DHCP Snooping实验配置步骤

```

Switch(config)# ip dhcp snooping //启用 DHCP Snooping
Switch(config)# ip dhcp snooping information option //启用 82 选项
//82 选项的功能：将 DHCP 请求发给 DHCP 服务器之前，Supervisor Engine 将向数据包中增加入口模块、端口、VLAN 和、交换机 MAC 地址
Switch(config-if)# ip dhcp snooping trust //配置信任端口
Switch(config)# ip dhcp snooping vlan //DHCP 监听作用的 VLAN
Switch# show ip dhcp snooping

```

2.11.4. IPSG (IP的源防护)

IPSG 能够提供检测机制来确保单个接口所接收到的数据包能够被各个接口所接收。如果检查成功通过，那么就将许可数据包；否则就会发生违背策略的活动。IPSG 不仅能够确保第 2 层网络中终端设备的 IP 地址不会产生冲突或占用，而且还能确保非授权的设备不能够通过自己指定的 IP 地址的方式来访问网络或导致网络不正常状态。

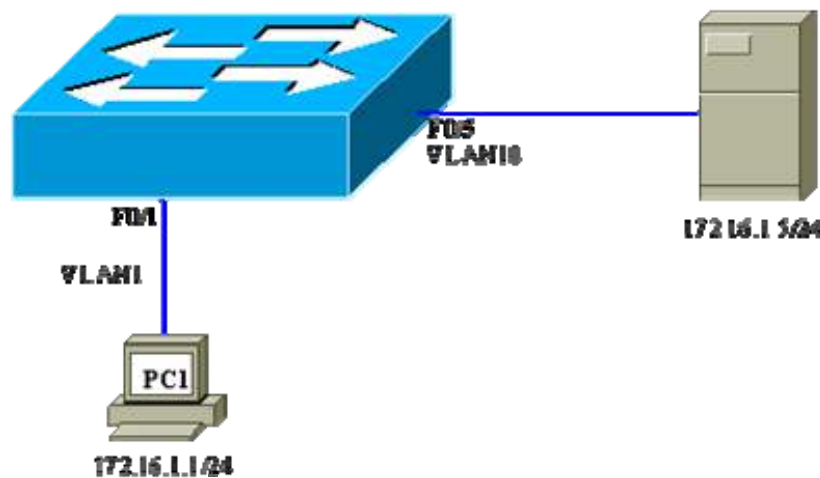
IPSG 实验配置步骤

```
SW2(config)# ip dhcp snooping
SW2(config)# ip dhcp snooping vlan 1
SW2(config)# interface range f0/2-3
SW2(config-if-range)# ip verify source port-security
SW2(config-if-range)# end
SW1(config)# ip source binding 00B0.6451.C920 vlan 1 172.1.1.51 interface Fa0/1 //可选配
SW1(config)# ip source binding 0007.EB5D.B0C0 vlan 1 172.1.1.52 interface Fa0/1 //可选配
```

IP 源防护实验

实验目的：只当由 DHCP SERVER 分配给 PC 机的地址才可正常访问网络，确保接入源的安全性。

说明：Cisco 2950 交换机不支持 IP 源防护功能，Cisco 2960 或 35 系列三层以上的交换机可支持该功能



```
SW(config)# ip dhcp snooping
SW(config)# ip dhcp snooping vlan 1,10
SW(config)# ip dhcp snooping verify mac-address
SW(config)# ip source binding 0000.0000.0001 vlan 10 172.16.1.5 interface f0/5
SW(config)# interface f0/1
SW(config-if)# switchport mode access
SW(config-if)# switchport port-security
SW(config-if)# ip verify source vlan dhcp-snooping port-security
SW(config)# interface f0/5
SW(config-if)# switchport mode access
SW(config-if)# switchport port-security
SW(config-if)# ip verify source vlan dhcp-snooping port-security
SW(config-if)# end
```



```
SW# show ip source binding
```

```
SW# show ip verify source
```

2.12. DAI(动态ARP检测)

2.12.1. DAI(动态ARP检测)

ARP(地址解析协议)的绑定

PC 机静态 ARP 绑定:

```
C:> ARP -s 192.168.1.1 00-50-8b-f0-0c-3e //ARP 静态绑定
```

```
C:> ARP -d //清除当前 ARP 列表
```

```
C:> ARP -a //查看当前所有 ARP 列表
```

Router 的静态 ARP 绑定:

```
Router(config)# arp 192.168.2.69 0001.1111.1111 arpa e0/0 //绑定
```

```
Router# show arp //查看 ARP 列表
```

```
Router# clear arp-cache //清除 ARP 列表
```

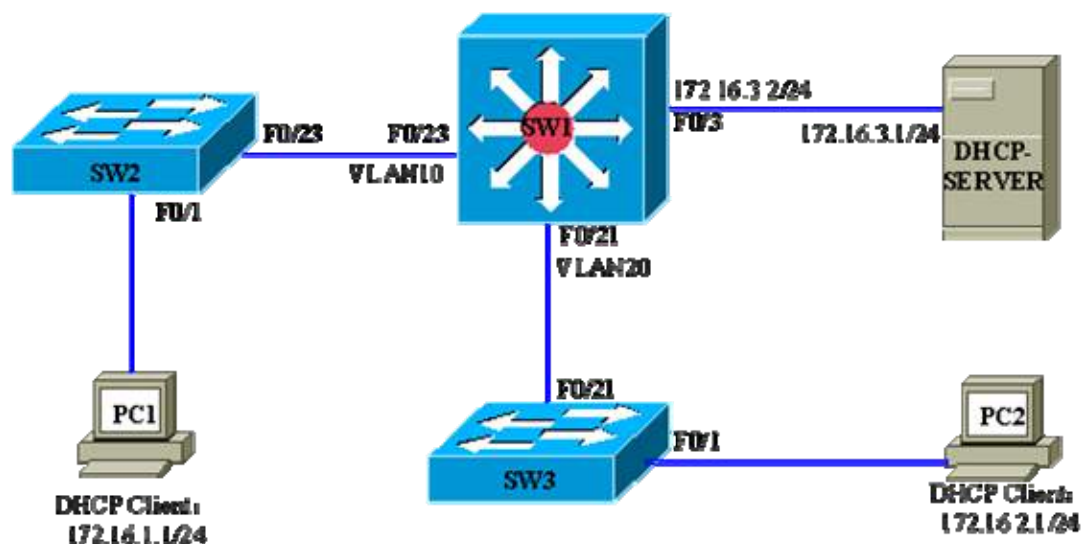
2.12.2. DAI的作用

DAI 是一种能够验证网络中 ARP 数据包的安全特性的一项技术。

虽然 dhcp snooping 是用来防止非法的 dhcp server 接入的,但是它一个重要作用是一旦客户端获得一个合法的 dhcp offer。启用 dhcp snooping 设备会在相应的接口下面记录所获得 IP 地址和客户端的 mac 地址。这个是后面另外一个技术 ARP inspection 检测的一个依据。ARP inspection 是用来检测 arp 请求的,防止非法的 ARP 请求。认为是否合法的标准的是前面 dhcp snooping 时建立的那张表。因为那种表是 dhcp server 正常回应时建立起来的,里面包括是正确的 arp 信息。如果这个时候有 arp 攻击信息,利用 ARP inspection 技术就可以拦截到这个非法的 arp 数据包。其实利用这个方法,还可以防止用户任意修改 IP 地址,造成地址冲突等问题。

2.12.3. 配置SW1 的防护功能

综合实验拓扑图及配置



```
SW1(config)# ip dhcp snooping
// 启用
```

DHCP Snooping

SW1(config)# ip dhcp snooping information option //启用 82 选项

SW1(config)# ip dhcp snooping vlan 10,20 //DHCP 监听作用的 VLAN

SW1(config)# ip dhcp database flash:dhcp.db //将 DHCP 绑定信息保存到 dhcp.db 中

SW1(config)# ip dhcp snooping verify mac-address

SW1(config)# interface f0/21

SW1(config-if)# switchport mode access

SW1(config-if)# switchport port-security

SW1(config-if)# ip verify source port-security

SW1(config)# interface f0/23

SW1(config-if)# switchport mode access

SW1(config-if)# switchport port-security

SW1(config-if)# ip verify source port-security

可选配//SW1(config)# ip source binding 0000.0000.0001 vlan 10 172.16.1.1 interface f0/2

可选配//SW1(config)# ip source binding 0000.0000.0002 vlan 20 172.16.2.1 interface f0/1

SW1(config)# ip arp inspection vlan 10,20 //ARP 检测基于 VLAN10 VLAN20

SW1(config)# ip arp inspection validate src-mac dst-mac ip //基于源 MAC 目标 MAC 和 IP

//DHCP 服务器的配置

DHCP-SERVER 使用路由器来完成

Router(config)# ip dhcp pool vlan10 定义地址池

Router(config-vlan)# network 172.16.1.0 255.255.255.0 定义地址池做用的网段及地址范围

Router(config-vlan)# default-router 172.16.1.254 定义客户端的默认网关

Router(config-vlan)# dns-server 218.108.248.200 定义客户端的 dns

Router(config-vlan)#exit

Router(config)# ip dhcp pool vlan20

Router(config-vlan)# network 172.16.2.0 255.255.255.0

Router(config-vlan)# default-router 172.16.2.254

Router(config-vlan)# dns-server 218.108.248.200

Router(config-vlan)# exit

Router(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.254 //配置保留地址段

Router(config)# ip dhcp excluded-address 172.16.2.100 172.16.2.254

Router(config)# interface e0/0

Router(config-if)# ip address 172.16.3.1 255.255.255.0

Router(config-if)# no shutdown

Router(config)# ip route 0.0.0.0 0.0.0.0 172.16.3.2 //配置回指路由

交换机上的配置

SW1(config)# interface vlan 10

SW1(config-if)# ip address 172.16.1.254 255.255.255.0

SW1(config-if)# ip helper-address 172.16.3.1 //以单播向 DHCP-SERVER 发送请求

SW1(config-if)# interface vlan20

SW1(config-if)# ip address 172.16.2.254 255.255.255.0

```
SW1(config-if)# ip helper-address 172.16.3.1
```

2.13. 创建多用户授权

2.13.1. 关于用户帐号的安全级别（1-15）

Level 1: 具有用户权限(Router>) 简单的查看功能

Level 15: 超级用户权限(Router#) 具有所有功能

Level 2 ---- Level 14 : 自定义用户权限 (Router#) 具有特定授权命令的功能

2.13.2. 创建用户

```
Router(config)# username test001 privilege 15 secret cisco001 //创建 15 级帐号
```

```
Router(config)# username test002 privilege 9 password cisco002 //创建 9 级帐号
```

```
Router(config)# username test003 password cisco003 //创建 1 级帐号
```

```
Router# show privilege //查看当前用户的安全级别
```

2.13.3. 给自定义用户授予命令权限

```
Router(config)# privilege 模式 级别 命令
```

➤ 配置特权模式的授权命令

```
Router(config)# privilege exec level 9 show run
```

```
Router(config)# privilege exec level 9 ping
```

```
Router(config)# privilege exec level 9 config ter
```

➤ 配置全局模式的授权命令

```
Router(config)# privilege configure level 9 ip route
```

```
Router(config)# privilege configure level 9 router
```

```
Router(config)# privilege configure level 9 interface
```

```
Router(config)# privilege configure level 9 line
```

➤ 配置接口模式下的授权命令

```
Router(config)# privilege interface level 9 ip address
```

```
Router(config)# privilege interface level 9 shutdown
```

```
Router(config)# privilege interface level 9 encapsulation
```

测试各用户的登陆权限方法，使用 VTY 登陆

```
Router(config)# line vty 0 15
```

```
Router(config-line)# login local //采用本地用户名和密码方式验证
```

```
Router(config-line)# end
```

测试结果：使用创建的帐号实施远程登陆

2.14. AAA

2.14.1. AAA

网络安全服务 AAA 提供了有关在 Cisco 交换机上配置访问控制的基本框架。AAA 是一个体系的结构框架，用于以统一的方式配置三种独立的安全功能。AAA 提供了一种完成下述服务的模块方法：

- Authentication 认证
功能：用户身份的认证、登陆和口令的对话、消息的接发和加密等
- Authorization 授权
功能：一次性授权和针对每种服务的授权，这是根据用户账户或用户组进行的
- Accounting 记帐(或叫统计)
功能：对于用户身份信息、登陆的时间、执行的命令、数据包等信息做记录

在很多情况下，AAA 使用诸如 RADIUS、TACACS+的服务器来提供通信；

CISCO 的软件有一块叫：ACS 的软件，可以提供 RADIUS 和 TACACS+的服务

以下的配置不包括在 ACS 服务器上的配置功能，只是作为 AAA 客户端的接入配置信息

- 客户端配置用户身份认证：

```
SW(config)# aaa new-model      //启用 AAA
SW(config)# aaa authentication login default local    // 采用本地数据库认证
SW(config)# aaa authentication login default group tacacs+ local  //先 tacacs+ 后 local
SW(config)# tacacs-server host 192.168.2.200 key cisco123
```

- 客户端配置用户的授权：

```
SW(config)# aaa new-model
SW(config)# aaa authorization commands 1 default group tacacs+ local
SW(config)# aaa authorization commands 15 default group tacacs+ local
SW(config)# line vty 0 4
SW(config-line)# authorization commands 1 default
SW(config-line)# authorization commands 15 default
```

- 客户端配置用户的记帐：

```
SW(config)# aaa new-model
SW(config)# aaa accounting exec default start-stop group tacacs+
SW(config)# aaa accounting commands 0 default start-stop group tacacs+
SW(config)# aaa accounting commands 1 default start-stop group tacacs+
SW(config)# aaa accounting commands 15 default start-stop group tacacs+
SW(config)# line vty 0 4
SW(config-line)# accounting exec default
SW(config-line)# accounting commands 0 default
SW(config-line)# accounting commands 1 default
SW(config-line)# accounting commands 15 default
```

特别说明：在配置 AAA 的时候，因为用户可能意外地将自己锁定到路由器或交换机的外部，所以应当特别谨慎，提前配置和管理员帐户和密码信息，否则用户将不得不通过口令恢复过程返回到

初始状态。

2.15. SNMP简单网络管理协议

2.15.1. SNMP简单网络管理协议

SNMP 是管理网络设备的标准协议，在中小型企业网络中，最适于针对于网络设备的工作状态监控。在大型企业网络规模中，使用 SNMP 可以集中管理和配置网络中的多层交换网络也是非常适用的。(CISCO 的网管软件叫：CiscoWorks H3C 的叫：Quidview 等)

使用这些 SNMP 的软件可以实现如下功能：

- 界面化配置和管理网络设备
- 接口链路的状态变化的报警和跟踪信息
- 接口的流量统计和性能报告
- 生成数据报表

要将交换机(或其它网络设备)启用 SNMP 协议并和网管软件相连，需要做以下的配置：

```
SW(config)# cdp run //启用 CDP 协议
```

```
SW(config)# snmp-server community zltrain ro //配置本路由器的只读字串为 zltrain
```

```
SW(config)# snmp-server community secret rw //配置本路由器的读写字串为 zltrain
```

```
SW(config)# snmp-server enable traps //允许路由器将所有 类型 SNMP Trap 发送出去
```

```
SW(config)# snmp-server host 192.168.1.200 rw //指定 SNMP 的管理服务器地址
```

```
SW(config)# end
```

3. CCNP ISCW课程

3.1.DSL技术

3.1.1. 概念：

DSL 技术是一种： 使用普通铜质电话线中未被使用的带宽来快速传输数字数据。其频率上限为 1MHZ。

- ADSL: 非对称数字用户线,下行速率比上行速率高
- SDSL: 对称数字用户线,上行速率和下行速率一样
- POTS: 电话服务网
- IDSL: 运行在 ISN 上的 DSL,速度为 144kbit/s

3.1.2. DSL技术的比较

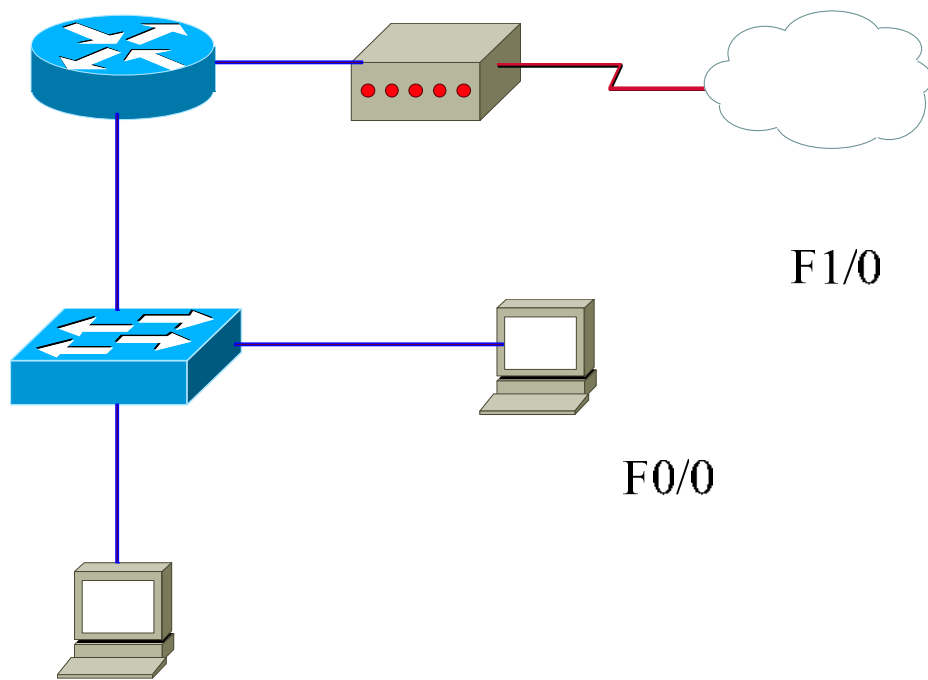
DSL Technology	Nature	Max. Data Rate (Down / Up) [bps]	Data and POTS
ADSL (非对称数字用户线)	Asymmetric	8 M / 1 M	Yes
VDSL (甚高速数字用户线)	Symmetric / Asymmetric	52 M / 13 M	Yes
IDSL (ISDN 数字用户线)	Symmetric	144 k / 144 k	No
SDSL (对称数字用户线)	Symmetric	768 k / 768 k	No
HDSL (高速数字用户线)	Symmetric	2 M / 2 M	No
G.SHDSL (单对高速率数字用户线)	Symmetric	2.3 M / 2.3 M	No

3.1.3. DSL的数据传输距离的比较

DSL Technology	Max. Data Rate (Down / Up) [bps]	Max. Distance [feet / km]
ADSL	8 M / 1 M	18,000 / 5.46
VDSL	52 M / 13 M	4,500 / 1.37
IDSL	144 k / 144 k	18,000 / 5.46
SDSL	768 k / 768 k	22,000 / 6.7
G.SHDSL	2.3 M / 2.3 M	28,000 / 8.52

3.1.4. 使用路由器做PPPoE的客户端连接

实验目的：使用路由器做 ADSL 的接入，可以正常给内网不同 VLAN 之间的 PC 机提供访问 Internet 服务



F1/0

F0/0

MODI

F0/1

F0/3

VLAN20

路由器配置:

Router(config)# interface FastEthernet0/0 //内网接口

Router(config-if)# no shutdown

Router(config)# interface FastEthernet0/0.10

Router(config-if)# encapsulation dot1q 10

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# ip nat inside

F0/2

VLAN10

Router(config)# interface FastEthernet0/0.20

Router(config-if)# encapsulation dot1q 20

Router(config-if)# ip address 192.168.2.1 255.255.255.0

Router(config-if)# ip nat inside

Router(config)# interface FastEthernet1/0 //连接 Modem 的以太网接口

Router(config-if)# pppoe enable

Router(config-if)# pppoe-client dial-pool-number 33

Router(config)# interface Dialer1

192.168.1.11

Router(config-if)# mtu 1492

Router(config-if)# ip address negotiated //地址获得方式为自动协商

Router(config-if)# ip nat outside //指定外部网络

Router(config-if)# encapsulation ppp //启用 ppp 封装协议

Router(config-if)# dialer pool 33 //调用 F1/0 为拨号接口

Router(config-if)# dialer-group 12 //跟 dialer-list 匹配,允许 IP 流通过

Router(config-if)# ppp authentication pap callin //启用 ppp 的验证方式为: pap

```
Router(config-if)# ppp pap sent-username hzhz89910961 password 654321 //宽带帐号和密码
```

```
Router(config)# ip route 0.0.0.0 0.0.0.0 Dialer1 //配置缺省路由
```

```
Router(config)# dialer-list 12 protocol ip permit
```

```
Router(config)# ip nat inside source list 45 interface Dialer1 overload //基于 PAT 的地址转换
```

```
Router(config)# access-list 45 permit 192.168.0.0 0.0.255.255
```

```
Router(config)# ip dhcp pool vlan10 //创建 DHCP 池
```

```
Router(chcp-config)# network 192.168.1.0 255.255.255.0
```

```
Router(chcp-config)# default-router 192.168.1.1
```

```
Router(chcp-config)# dns-server 218.108.248.200 202.101.172.46
```

```
Router(config)# ip dhcp pool vlan20 //创建 DHCP 池
```

```
Router(chcp-config)# network 192.168.2.0 255.255.255.0
```

```
Router(chcp-config)# default-router 192.168.2.1
```

```
Router(chcp-config)# dns-server 218.108.248.200 202.101.172.46
```

```
//设定保留地址段(可选)
```

```
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

```
Router(config)# ip dhcp excluded-address 192.168.1.200 192.168.1.254
```

```
Router(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
```

交换机实验配置

```
SW(Config)# interface F0/1
```

```
SW(config-if)# switchport trunk encapsulation dot1q
```

```
SW(config-if)# switchport mode trunk
```

```
SW(config)# vlan 10
```

```
SW(config)# vlan 20
```

```
SW(config)# interface f0/2
```

```
SW(config-if)# switchport access vlan 10
```

```
SW(config-if)# switchport mode access
```

```
SW(config)# interface f0/3
```

```
SW(config-if)# switchport access vlan20
```

```
SW(config-if)# switchport mode access
```

3.2. MPLS(多协议标签交换)

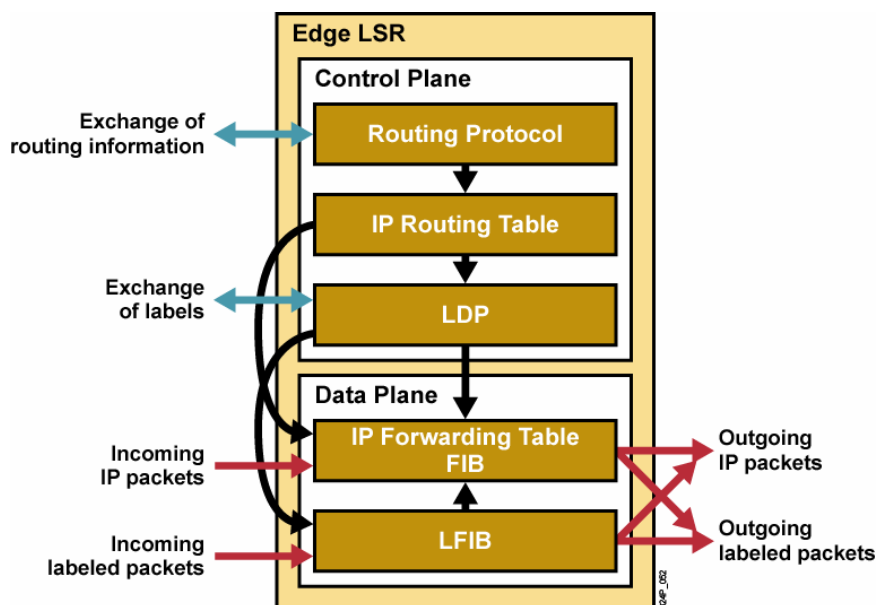
3.2.1. MPLS术语

- LSR 标签交换路由器
- Edge LSR 边缘的标签交换路由器
- Impose Label 压标签

- POP Label 标签弹出
- LDP 标签分发协议
- LFIB 标签转发信息表
- PHP 次末跳弹出(倒数第二跳弹出)
- CE 直接与 ISP 相连的用户端设备
- PE ISP 骨干网上的边缘路由器，与 CE 相连，主要负责 VPN 业务的接入
- P 指 ISP 骨干网上的核心路由器，主要完成标签和路由的快速转发

3.2.2. MPLS的架构

- 控制面板(Control plane)
 - a. 交换路由信息和标签信息
 - b. 包含的是各种 IP 路由协议 OSPF EIGRP RIP BGP ISIS
 - c. 交换标签协议: LDP
- 数据面板(Data plane)
 - a. 数据包的转发是基于标签的
 - b. 拥有简单的转发引擎
 - c. 操作方法为:
 - 1) 收到纯 IP 报文，转发为标签报文
 - 2) 收到标签报文，转发为 IP 报文
 - 3) 收到标签报文，转发标签报文
 - 4) 收到纯 IP 报文，转发 IP 报文

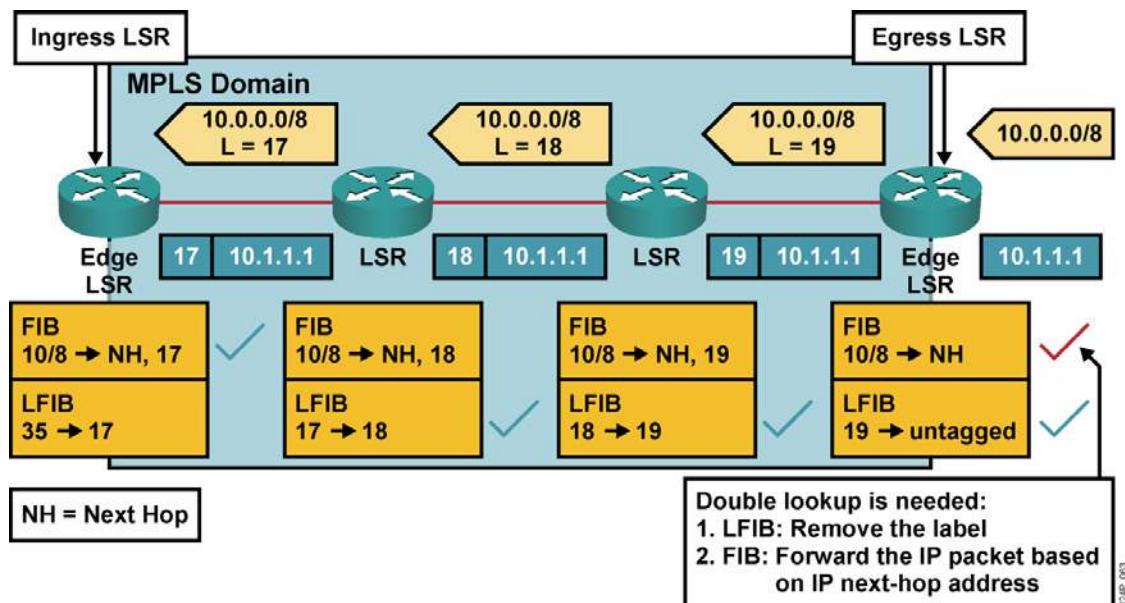


3.2.3. PHP(倒数第二跳弹出)

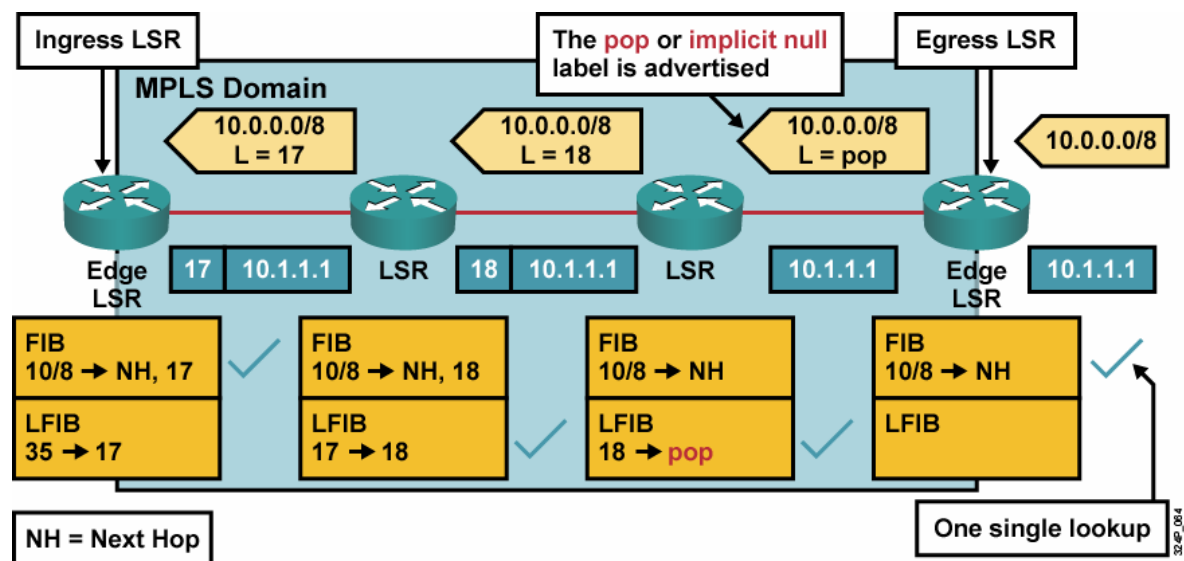
Egress LSR 本应变 MPLS 转发为 IP 路由查找，但是他收到的仍旧是含有标签的 MPLS 报文，按照常规，这个报文应该送交 MPLS 模块处理，而此时 MPLS 模块不需要标签转发，能做的只是去掉标签，然后送交 IP 层。其实对于 Egress LSR，处理 MPLS 报文是没有意义的。最好能够保证他直接收到的就是 IP 报文。这就需要在 Edge LSR 的上游（倒数第二跳）就把标签给弹出来。但关键问题是：上游设备如何知道自己是倒数第二跳呢？其实很简单，在倒数第一跳为其分配标签

时做一下特殊说明即可（分配一个特殊的标签 3）

没采用 PHP 之前的示例图

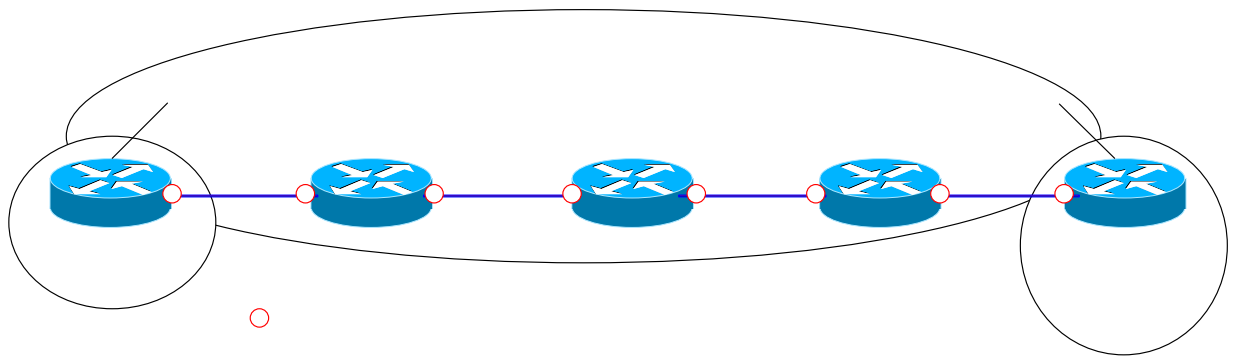


采用了 PHP 之后的示例图



3.2.4. MPLS转发实验

实验目的：使用 MPLS 穿越 BGP 路由黑洞，实现 BGP 的路由可达性



EIGRP

实验的测试结果是能够实现：在 R1 上面可以 ping 通 R5 上的 BGP 路由 50.50.1.1、2.2、3.3 等

R1 的配置

```
R1(config)# interface F0/0
```

```
R1(config-if)# ip address 12.0.0.1 255.255.255.0
```

```
R1(config-if)# mpls ip //启用 MPLS 转发 F0/0 F0/0
```

```
R1(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
```

```
R1(config-if)# exit 12.0.0.0/24
```

F1/0 F1/0

23.0.0.0/24

```
R1(config)# interface loopback 0
```

```
R1(config-if)# ip address 1.1.1.1 255.255.255.255
```

```
R1(config)# router eigrp 100 AS 101
```

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

```
R1(config-router)# network 12.0.0.0
```

```
R1(config-router)# network 1.0.0.0
```

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

```
R1(config)# router bgp 101
```

```
R1(config-router)# neighbor 5.5.5.5 remote-as 101
```

```
R1(config-router)# neighbor 5.5.5.5 update-source loopback 0
```

```
R1(config-router)# neighbor 5.5.5.5 next-hop-self
```

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

表示接口下运行MPLS

R2 的配置

```
R2(config)# interface F0/0
```

```
R2(config-if)# ip address 12.0.0.2 255.255.255.0
```

```
R2(config-if)# mpls ip //启用 MPLS 转发
```

```
R2(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
```

```
R2(config-if)# interface F1/0
```

```
R2(config-if)# ip address 23.0.0.2 255.255.255.0
```

```
R2(config-if)# mpls ip //启用 MPLS 转发
```

```
R2(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
```

```
R2(config)# router eigrp 100
```

```
R2(config-router)# no auto-summary
```

```
R2(config-router)# network 12.0.0.0
```

```
R2(config-router)# network 23.0.0.0
```

```
R2(config-router)# end
```

R3 的配置

```
R3(config)# interface F0/0
R3(config-if)# ip address 34.0.0.3 255.255.255.0
R3(config-if)# mpls ip //启用 MPLS 转发
R3(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
R3(config-if)# interface F1/0
R3(config-if)# ip address 23.0.0.3 255.255.255.0
R3(config-if)# mpls ip //启用 MPLS 转发
R3(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
R3(config)# router eigrp 100
R3(config-router)# no auto-summary
R3(config-router)# network 34.0.0.0
R3(config-router)# network 23.0.0.0
R3(config-router)# end
```

R4 的配置

```
R4(config)# interface F0/0
R4(config-if)# ip address 34.0.0.4 255.255.255.0
R4(config-if)# mpls ip //启用 MPLS 转发
R4(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
R4(config-if)# interface F1/0
R4(config-if)# ip address 45.0.0.4 255.255.255.0
R4(config-if)# mpls ip //启用 MPLS 转发
R4(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
R4(config)# router eigrp 100
R4(config-router)# no auto-summary
R4(config-router)# network 34.0.0.0
R4(config-router)# network 45.0.0.0
R4(config-router)# end
```

R5 的配置

```
R5(config)# interface F0/0
R5(config-if)# ip address 45.0.0.5 255.255.255.0
R5(config-if)# mpls ip //启用 MPLS 转发
R5(config-if)# mpls lable protocol ldp //启用 LDP 协议(默认)
R5(config-if)# exit
R5(config)# interface loopback 0
R5(config-if)# ip address 5.5.5.5 255.255.255.255
R5(config)# interface loopback 11
R5(config-if)# ip address 50.50.1.1 255.255.255.255 //发布 BGP 中，模拟互联网 BGP 路由
R5(config)# interface loopback 12
R5(config-if)# ip address 50.50.2.2 255.255.255.255 //发布 BGP 中，模拟互联网 BGP 路由
R5(config)# interface loopback 13
R5(config-if)# ip address 50.50.3.3 255.255.255.255 //发布 BGP 中，模拟互联网 BGP 路由

R5(config)#router eigrp 100
R5(config-router)# no auto-summary
```

```

R5(config-router)# network 45.0.0.0
R5(config-router)# network 5.0.0.0
R5(config-router)# exit
R5(config)# router bgp 101
R5(config-router)# neighbor 1.1.1.1 remote-as 101
R5(config-router)# neighbor 1.1.1.1 update-source loopback 0
R5(config-router)# neighbor 1.1.1.1 next-hop-self
R5(config-router)# network 50.50.1.1 mask 255.255.255.255
R5(config-router)# network 50.50.2.2 mask 255.255.255.255
R5(config-router)# network 50.50.3.3 mask 255.255.255.255
R5(config-router)# end

```

相关查看命令

```

R1#show mpls ldp neighbor //查看 LDP 的邻居信息
    Peer LDP Ident: 23.0.0.2:0; Local LDP Ident 1.1.1.1:0
    TCP connection: 23.0.0.2.30697 - 1.1.1.1.646
    State: Oper; Msgs sent/rcvd: 36/39; Downstream
    Up time: 00:24:32
    LDP discovery sources:
    FastEthernet0/0, Src IP addr: 12.0.0.2
    Addresses bound to peer LDP Ident:
    12.0.0.2      23.0.0.2

```

```

R1#show mpls ip binding //查看 LIB 表
    1.1.1.1/32
    in label:      imp-null
    out label:     17      lsr: 23.0.0.2:0
    5.5.5.5/32
    in label:      17
    out label:     18      lsr: 23.0.0.2:0      inuse
    .....

```

```

R1#show ip cef detail //查看 CEF 信息表及标签分发信息
5.5.5.5/32, version 14, epoch 0, cached adjacency 12.0.0.2
0 packets, 0 bytes
    tag information set, shared
    local tag: 17
    fast tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}
    via 12.0.0.2, FastEthernet0/0, 3 dependencies
    next hop 12.0.0.2, FastEthernet0/0
    valid cached adjacency
    tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}
50.50.1.1/32, version 15, epoch 0, cached adjacency 12.0.0.2
0 packets, 0 bytes
    tag information from 5.5.5.5/32, shared
    local tag: 17

```

fast tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}
 via 5.5.5.5, 0 dependencies, recursive
 next hop 12.0.0.2, FastEthernet0/0 via 5.5.5.5/32
 valid cached adjacency
 tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}
 50.50.2.2/32, version 16, epoch 0, cached adjacency 12.0.0.2
 0 packets, 0 bytes
 tag information from 5.5.5.5/32, shared
 local tag: 17
 fast tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}
 via 5.5.5.5, 0 dependencies, recursive
 next hop 12.0.0.2, FastEthernet0/0 via 5.5.5.5/32
 valid cached adjacency
 tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}
 50.50.3.3/32, version 17, epoch 0, cached adjacency 12.0.0.2
 0 packets, 0 bytes
 tag information from 5.5.5.5/32, shared
 local tag: 17
 fast tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}
 via 5.5.5.5, 0 dependencies, recursive
 next hop 12.0.0.2, FastEthernet0/0 via 5.5.5.5/32
 valid cached adjacency
 tag rewrite with Fa0/0, 12.0.0.2, tags imposed: {18}

R1#show mpls forwarding-table //查看 LFIB 表

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	16	34.0.0.0/24	0	Fa0/0	12.0.0.2
17	18	5.5.5.5/32	0	Fa0/0	12.0.0.2
18	Pop tag	23.0.0.0/8	0	Fa0/0	12.0.0.2
19	19	45.0.0.0/24	0	Fa0/0	12.0.0.2

R2#show mpls forwarding-table

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	34.0.0.0/24	0	Fa1/0	23.0.0.3
17	Pop tag	1.1.1.1/32	2171	Fa0/0	12.0.0.1
18	17	5.5.5.5/32	8117	Fa1/0	23.0.0.3
19	19	45.0.0.0/24	0	Fa1/0	23.0.0.3

R3#show mpls forwarding-table

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	17	1.1.1.1/32	2368	Fa1/0	23.0.0.2
17	17	5.5.5.5/32	8632	Fa0/0	34.0.0.4
18	Pop tag	12.0.0.0/8	5171	Fa1/0	23.0.0.2

19	Pop tag	45.0.0.0/24	0	Fa0/0	34.0.0.4
----	---------	-------------	---	-------	----------

R4#show mpls forwarding-table

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	16	1.1.1.1/32	0	Fa0/0	34.0.0.3
17	Untagged	5.5.5.5/32	8447	Fa1/0	45.0.0.5
18	Pop tag	23.0.0.0/24	0	Fa0/0	34.0.0.3
19	18	12.0.0.0/8	0	Fa0/0	34.0.0.3

R1#traceroute 50.50.1.1

Type escape sequence to abort.

Tracing the route to 50.50.1.1

1	12.0.0.2 [MPLS: Label 18 Exp 0]	196 msec	100 msec	60 msec
2	23.0.0.3 [MPLS: Label 17 Exp 0]	24 msec	56 msec	28 msec
3	34.0.0.4 [MPLS: Label 17 Exp 0]	32 msec	44 msec	84 msec
4	45.0.0.5	148 msec	*	356 msec

R1#ping 50.50.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 50.50.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/77/176 ms

3.3. IPsec (IP的安全)

3.3.1. IPsec的基概念

IPsec 并不是协议，它是设计用来给网络层提供数据认证、数据完整性和数据机密性的开放式标准协议的框架。

- 认证(Authentication): 确定所接受的数据与所发送的数据是一致的，同时可以确定申请发送者在实际上是真实的发送者，而不是伪装的
- 数据的完整性(Data Integrity): 保证数据从原发地到目的地的传送过程中没有任何不可检测的数据丢失和改变
- 机密性(Confidentiality): 使相应的接收者能获取发送的真正内容，而无意获取数据的接收者无法获知数据的真正内容

3.3.2. IPsec的主要协议

- IKE(互联网密钥交换): 提供网络框架安全参数的协商，以及认证密钥的建立
- ESP(封装安全有效载荷): 提供数据的认证、数据完整性服务以及机密性服务
- AH(头部认证): 提供数据认证，以及完整性服务，可以对 IP 数据包的头部进行认证

3.3.3. 安全算法

- 加密算法：加密和解密数据的数学算法
 - 对称加密算法(DES 3DES AES)
 - 非对称加密算法(RSA)
- 散列算法：用来确保数据的完整性
 - HMAC： MD5 SHA-1
 - (关于 HMAC 的备注：hmac 主要应用在身份验证中，它的使用方法是这样的：
 - a. 客户端发出登录请求（假设是浏览器的 GET 请求）
 - b. 服务器返回一个随机值，并在会话中记录这个随机值
 - c. 客户端将该随机值作为密钥，用户密码进行 hmac 运算，然后提交给服务器
 - d. 服务器读取用户数据库中的用户密码和步骤 2 中发送的随机值做与客户端一样的 hmac 运算，然后与用户发送的结果比较，如果结果一致则验证用户合法)
- 认证方法：可以对用户的身份提供认证
 - 预共享密钥(Pre-shared key)
 - 数字签名(CA)
- DH 算法(Diffie-Hellman) /DH 组
 - 是一项公开密钥加密协议，其在两个 IPsec 对等实体之间使用以从一个不安全的隧道得到共享密钥，而不用将共享密钥在两个对等实体之间互相传输
 - DH-1: 768bit DH-2: 1024bit DH-5: 1536bit

3.3.4. IKE的工作阶段

Phase I：IKE 的第 1 阶段（IKE 的 SA 又称为：ISAKMP 的 SA）

- a. 对两个对等体之间提供认证
- b. 双向 SA(安全关联)参数的协商
- c. 工作在两种模式：主要模式和野蛮模式

说明：IKE 的第 1 阶段并不直接用来提供数据的加密

Phase II：IKE 的第 2 阶段（IPsec 的 SA）

- a. 针对于 ESP 或 AH 的参数协商
- b. 工作在：快速模式

说明：IKE 的第 2 阶段真正用来为数据提供加密

3.3.5. 关于ESP和AH

ESP：提供数据认证、机密性和完整性服务，主要负责以一种安全方式从到目的的资源获得数据，检验数据没有被改变，以及确保会话不会被截取。IP 协议号为：50，可以工作在基于 PAT(基于端口的 NAT)的网络中。

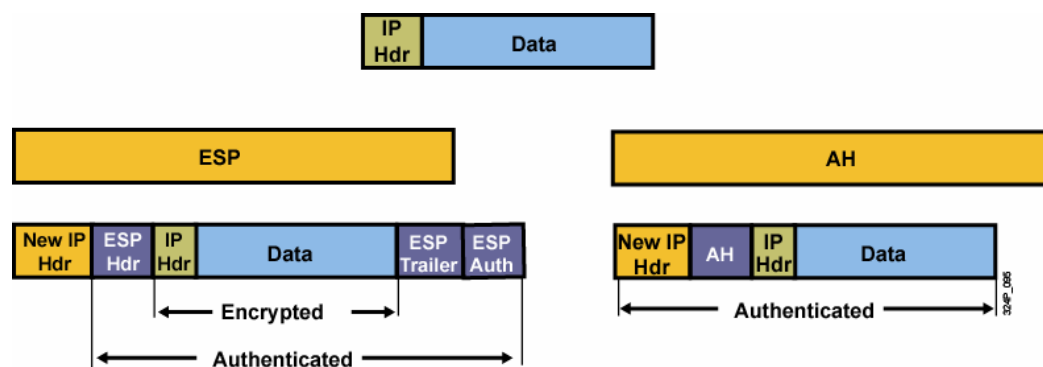
(ESP 的概念补充说明：封装安全负载（ESP）通过对数据包的全部数据和加载内容进行全加密来严格保证传输信息的机密性，这样可以避免其他用户通过监听来打开信息交换的内容，因为只有受信任的用户拥有密钥打开内容。ESP 也能提供认证和维持数据的完整性。最主要的 ESP 标准是数据加密标准（DES），DES 最高支持 56 位的密钥，而 Triple-DES 使用三套密钥加密，那就相当于使用最高到 168 位的密钥。由于 ESP 实际上加密所有的数据，因而它比 AH 需要更多的处

理时间，从而导致性能下降。)

AH: 提供数据的认证和完整性服务, AH 不提供任何数据的加密, 它仅提供起源认证或者检验来自发送器的数据, 能够防止会话被截取。IP 协议号为: 51, 不可以工作在基于 PAT 的网络。

(AH 的概念补充说明: 认证协议头 (AH) 是在所有数据包头加入一个密码。正如整个名称所示, AH 通过一个只有密钥持有人才知道的"数字签名"来对用户进行认证。这个签名是数据包通过特别的算法得出的独特结果; AH 还能维持数据的完整性, 因为在传输过程中无论多小的变化被加载, 数据包头的数字签名都能把它检测出来。不过由于 AH 不能加密数据包所加载的内容, 因而它不保证任何的机密性。两个最普遍的 AH 标准是 MD5 和 SHA-1, MD5 使用最高到 128 位的密钥, 而 SHA-1 通过最高到 160 位密钥提供更强的保护)

ESP 和 AH 的 IP 数据包头部模式比较



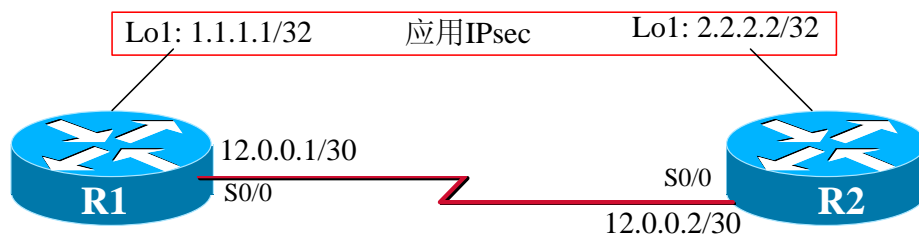
3.3.6. 关于隧道模式和传输模式

Tunnel mode 隧道模式: 通常当 ESP 在关联到多台主机的网络访问介入装置实现时使用, 隧道模式处理整个 IP 数据包--包括全部 TCP/IP 或 UDP/IP 头和数据, 它用自己的地址作为源地址加入到新的 IP 头。当隧道模式用在用户终端设置时, 它可以提供更多的便利来隐藏内部服务器主机和客户机的地址。

Transport mode 传送模式: 传送模式使用原始明文 IP 头, 并且只加密数据, 包括它的 TCP 和 UDP 头

七、配置 IPsec 的加密通道

实验目的: 针对定义的感兴趣流量, 提供加密, 应用 IPsec。对于非指定的流量, 全部按原有模式正常传输数据, 不提供任何加密, 不应用 IPsec。



说明: 当 R1 以源地址 1.1.1.1 访问目的地址 R2 的 2.2.2.2 的时候, 才会应用 IPsec, 否则其它的任何情况均不应用 IPsec。

R1 的配置

```

//定义互联网密钥管理协议的策略(ISAKMP 的策略)
//R1#sh crypto isakmp policy    //查看路由器的默认策略

R1(config)# crypto isakmp policy 1 //进入 IKE 策略编辑模式,数字越小被能优先使用
R1(config-isakmp)# authentication pre-share //使用预共享密钥
R1(config-isakmp)# encryption 3des //加密方式为 3DES
R1(config-isakmp)# hash md5 //散列算法,默认 SHA,路由器不够强大就使用 MD5
R1(config-isakmp)# group 2 //Diffie-Hellman 2 密钥交换方法
R1(config-isakmp)# lifetime 500 //IKE SA 生命周期,默认 86400 秒,也就是一天

//指定共享密钥的地址
R1(config)# crypto isakmp key 0 cisco address 12.0.0.2

//IPsec 转换集 进行对数据的交换进行加密
R1(config)# crypto ipsec transform-set TEST000 esp-3des esp-md5-hmac
!
//加密映射 设定对等体以及感兴趣的数据流
R1(config)# crypto map r1 10 ipsec-isakmp
R1(config-crypto-map)# set peer 12.0.0.2
R1(config-crypto-map)# set transform-set TEST000
R1(config-crypto-map)# match address 101 //匹配感兴趣数据流

R1(config)# access-list 101 permit ip host 1.1.1.1 host 2.2.2.2
R1(config)# ip route 2.2.2.2 255.255.255.255 12.0.0.2
R1(config)# interface Serial0/0
R1(config-if)# ip address 12.0.0.1 255.255.255.252
R1(config-if)# crypto map r1
R1(config-if)# end

R2 的配置
R2(config)# crypto isakmp policy 1 //进入 IKE 策略编辑模式,数字越小被能优先使用
R2(config-isakmp)# authentication pre-share //使用预共享密钥
R2(config-isakmp)# encryption 3des //加密方式为 3DES
R2(config-isakmp)# hash md5 //散列算法,默认 SHA,路由器不够强大就使用 MD5
R2(config-isakmp)# group 2 //Diffie-Hellman 2 密钥交换方法
R2(config-isakmp)# lifetime 500 //IKE SA 生命周期,默认 86400 秒,也就是一天

R2(config)# crypto isakmp key 0 cisco address 12.0.0.1
R2(config)# crypto ipsec transform-set TEST000 esp-3des esp-md5-hmac
R2(config)# crypto map R2 10 ipsec-isakmp
R2(config-crypto-map)# set peer 12.0.0.1
R2(config-crypto-map)# set transform-set TEST000
R2(config-crypto-map)# match address 101 //匹配感兴趣数据流

R2(config)# access-list 101 permit ip host 2.2.2.2 host 1.1.1.1
R2(config)# ip route 1.1.1.1 255.255.255.255 12.0.0.1

```

```
R2(config)# interface Serial0/0
R2(config-if)# ip address 12.0.0.2 255.255.255.252
R2(config-if)# crypto map R2
R2(config-if)# end

R2# debug crypto isakmp //打开 IKE 第一阶段的跟踪消息
R2# debug crypto ipsec //打开 IKE 第二阶段的跟踪消息
R2#undebug all //关闭所有跟踪消息
测试方法: R1# ping 2.2.2.2 source 1.1.1.1 //触发 IPsec
```

3.4. 站点VPN (Site to Site VPN)

3.4.1. 配置Cisco路由器支持SDM管理软件的连接

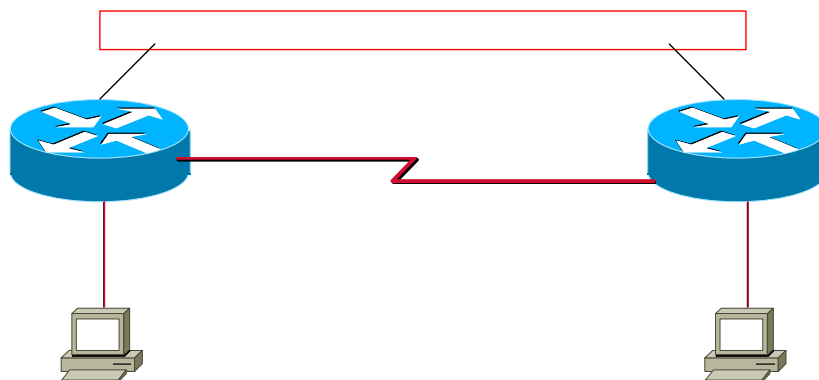
```
Router(config)# ip http server //启用 http 服务
Router(config)# line vty 0 4
Router(config-line)# login local
Router(config-line)# exit
Router(config)# username super001 privilege 15 password cisco
```

3.4.2. SDM软件的安装及需要修改的文件信息

进入安装目录: C:\Program Files\Cisco Systems\Cisco SDM_zh\common\common

- 1、将 runAPP.shtml 文件的扩展名修改为: runnAPP.html
- 2、用记事本打开 launchTask.html 文件,搜索 runAPP.shtml 字段,修改为:runnAPP.html , 保存退出即可。

3.4.3. 使用SDM工具配置 Site to Site VPN



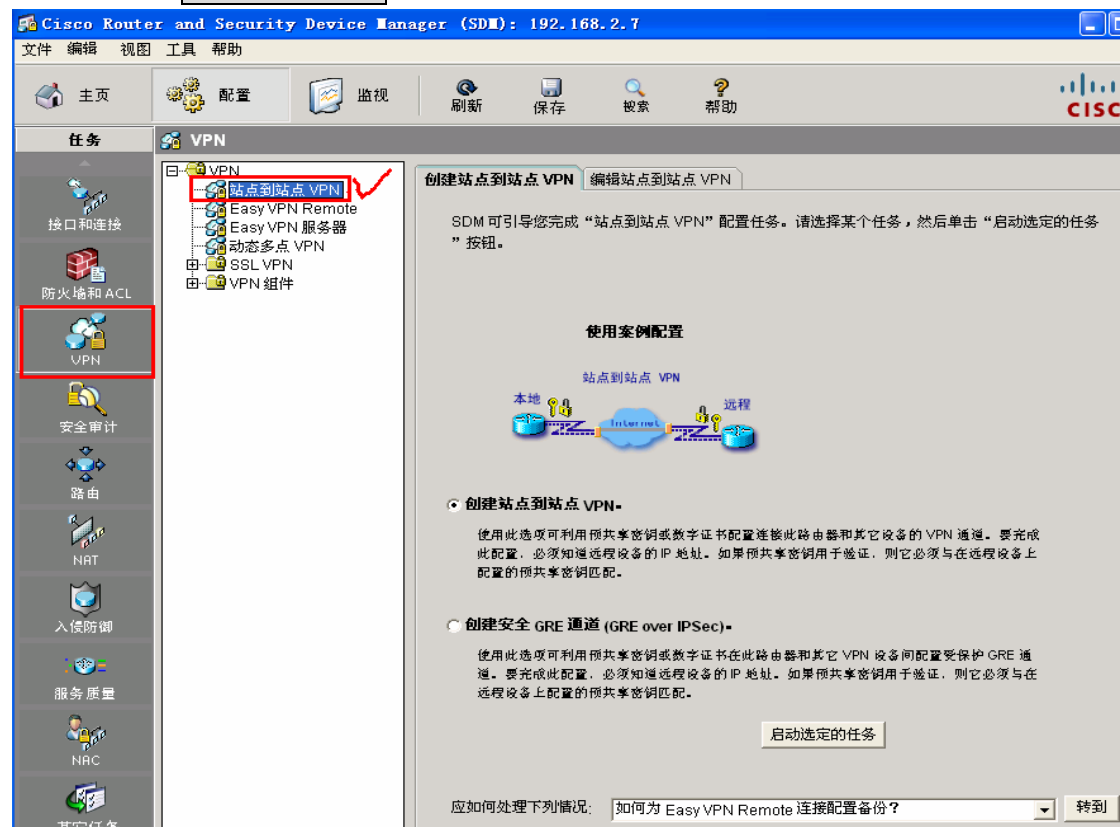
第 1 步 点击：主页面上的：**配置** 进入配置选项



第 2 步 在配置选项里面，点击 **VPN 选项**



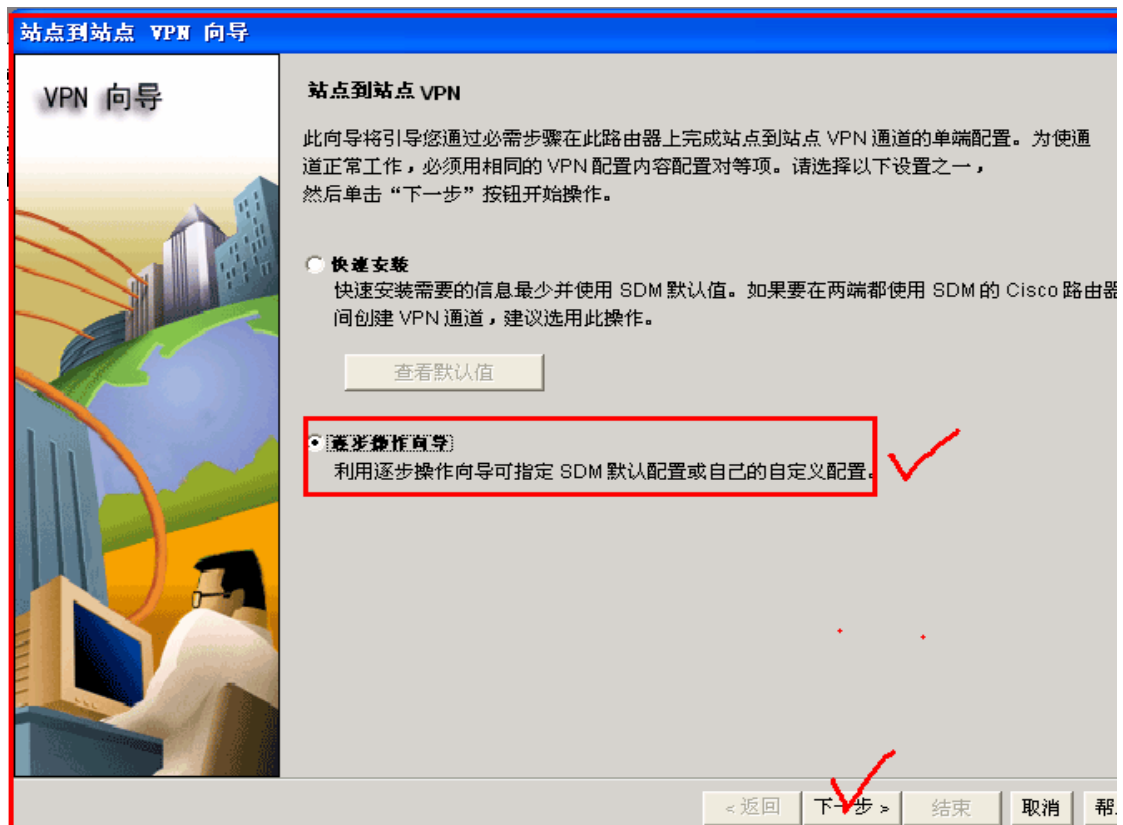
第 3 步 选择 **站点到站点 VPN**



第 4 步 点击: **创建站点到站点 VPN** 选项



第 5 步 使用 **逐步操作向导**，目的是可以自定义配置各种加密方法。



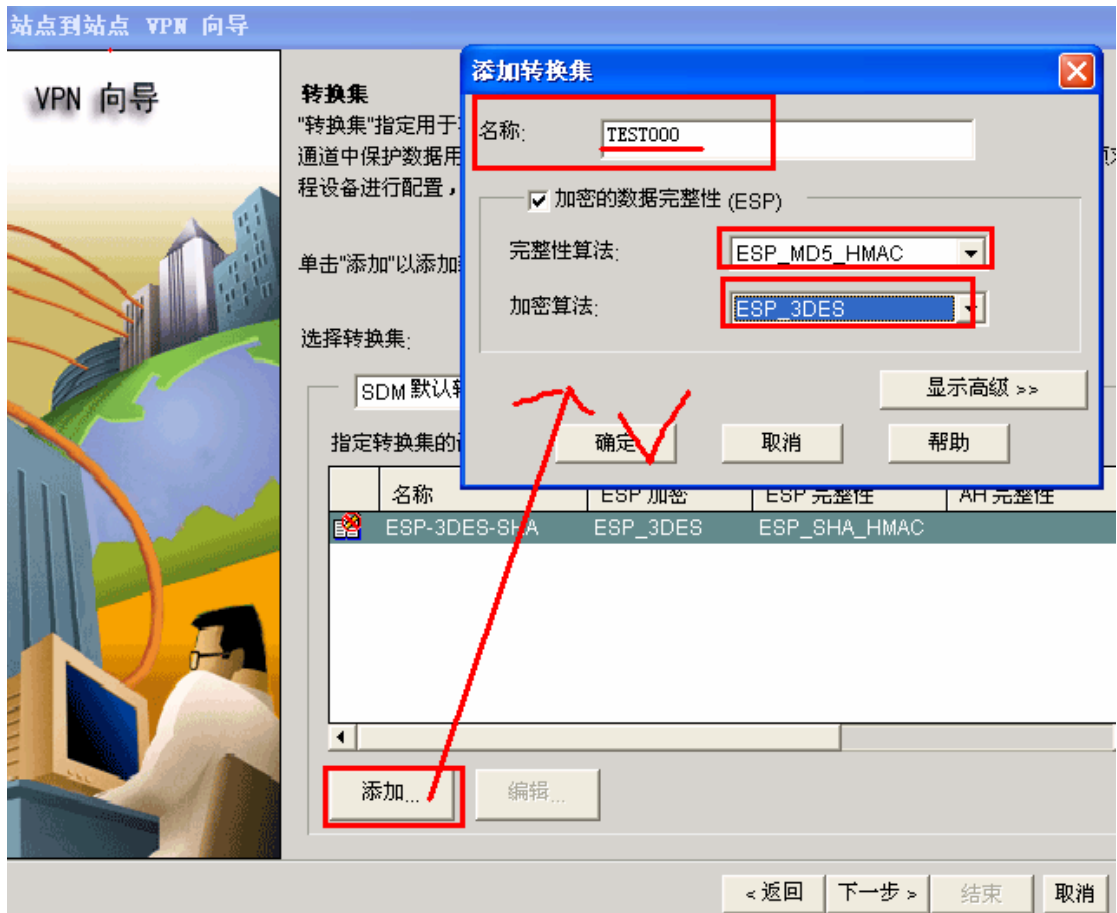
第 6 步 做 VPN 连接的接口及对端站点地址设置



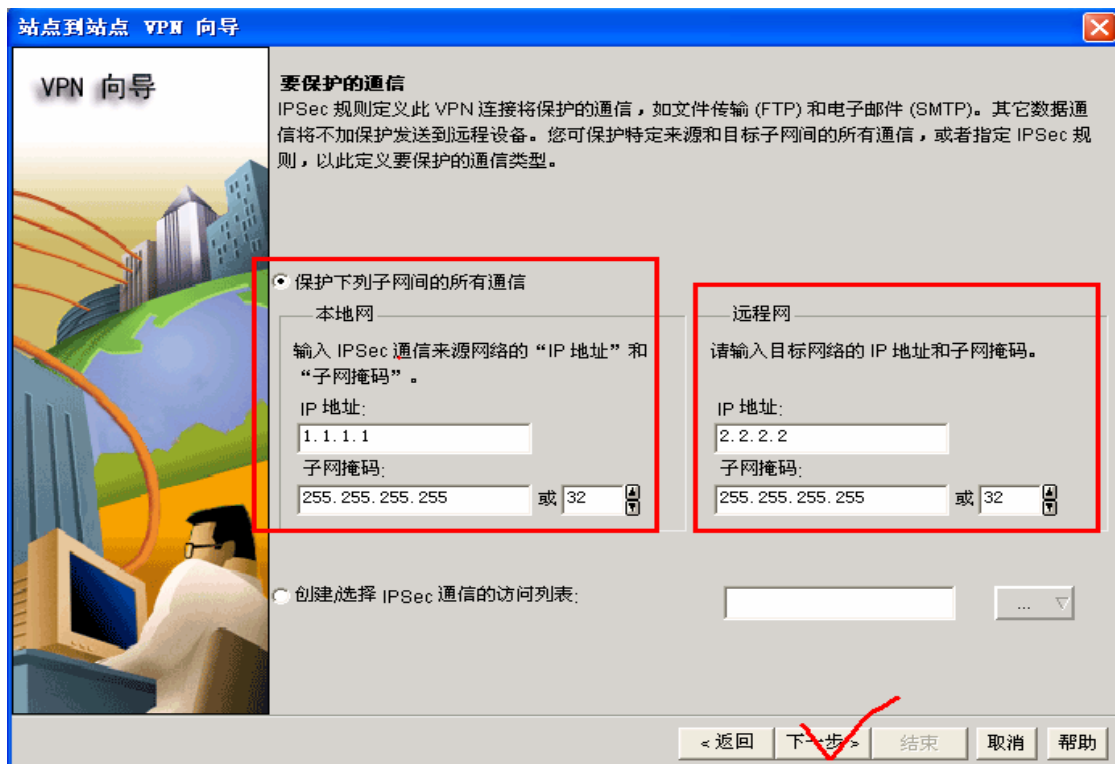
第 7 步 设定 IKE 的策略



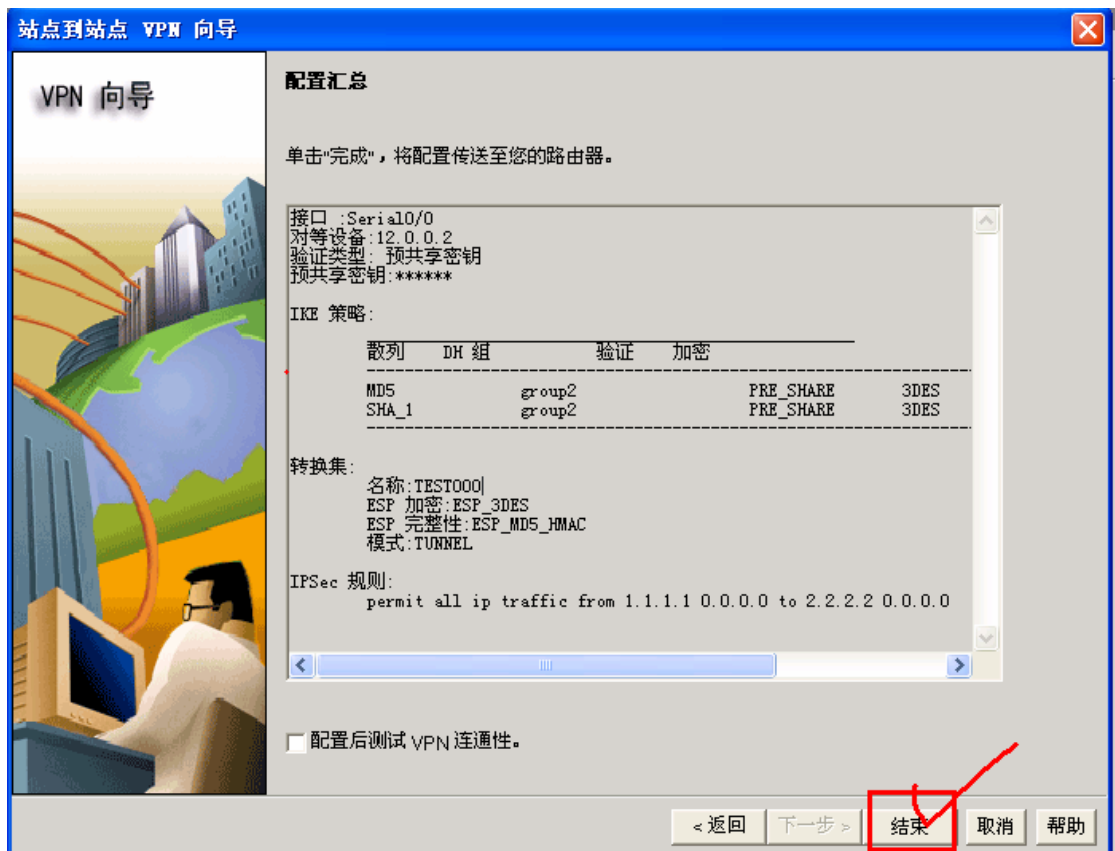
第 8 步 设定 transform-set 转换集的完整性算法和加密算法



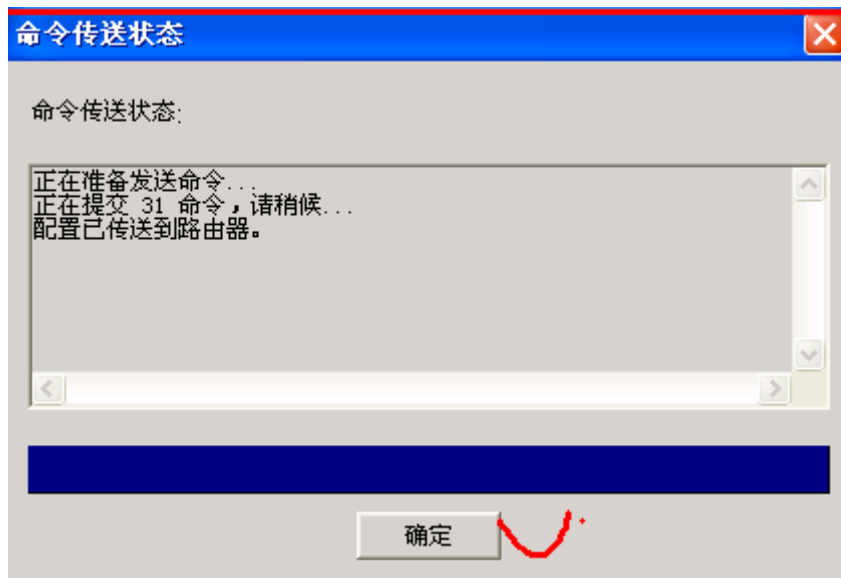
第 9 步 定义感兴趣数据流



第 10 步 完成配置，点击结束



第 11 步 最后可以看到命令提交成功即可。



说明：另一端路由器采用同样的方法做配置，注意修改 IP 地址、接口及对端站点等信息
测试方法可以进入路由器中使用

R1# ping 2.2.2.2 source 1.1.1.1

若可以 ping 通即可。实验完成。

3.5. GRE over IPsec 通用路由封装

3.5.1. GRE的基本概念

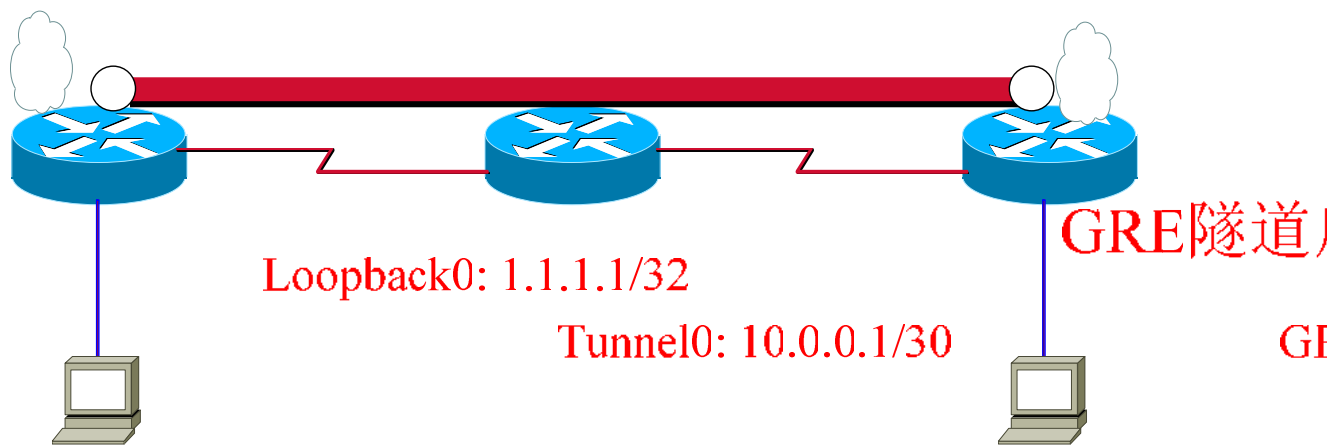
- GRE 的 Tunnel 隧道可以支持多个协议(IP、Appletalk、IPX)
- 建立的 Tunnel 提供了虚拟点到点的链路(是一条直连的虚拟链路)
- IP 的路由协议可以在 Tunnel 的隧道中传输
- Tunnel 默认不提供：认证、完整性和机密性服务，需 IPsec 支持。

3.5.2. GRE链路的配置要求

- 配置 Tunnel 接口虚链路地址
- 指定建立隧道的源地址，或源接口
- 指定建立隧道的目标地址，且目标地址一定是可达的
- 配置隧道工作模式。
- 若启用了 IPsec，则需要在 Tunnel 的接口应用 Crypto map

3.5.3. 使用SDM配置GRE over IPsec实验

实验图如下：



命令行模式下的配置：

R1 路由器命令配置

R1(config)# crypto isakmp policy 2

R1(config-isakmp)# encr 3des

R1(config-isakmp)# hash md5

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# group 2

R1(config)# crypto isakmp key cisco address 23.0.0.2

R1(config)# crypto ipsec transform-set TEST000 esp-3des esp-md5-hmac

R1(config)# crypto map R1 1 ipsec-isakmp

R1(config-crypto-map)# set peer 23.0.0.2

R1(config-crypto-map)# set transform-set TEST000

R1(config-crypto-map)# match address 100

SDM

R1(config)# interface Loopback0

R1(config-if)# ip address 1.1.1.1 255.255.255.255

R1(config)# interface Tunnel0

R1(config-if)# ip address 10.0.0.1 255.255.255.252

R1(config-if)# tunnel source Serial0/0

R1(config-if)# tunnel destination 23.0.0.2

R1(config-if)# crypto map R1

R1(config)# interface Serial0/0

R1(config-if)# ip address 12.0.0.1 255.255.255.252

R1(config)# interface FastEthernet1/0

R1(config-if)# ip address 192.168.3.91 255.255.255.0 //用于连接 PC 机，可使用 SDM 配置

R1(config)# router eigrp 10

R1(config-router)# network 12.0.0.0

R1(config-router)# no auto-summary

R1(config-router)# exit

R1(config)# router rip

R1(config-router)# version 2

R1(config-router)# network 1.0.0.0

12.0.0.1/30

S0/0

12.0.0.2/30

S0/0

EIGRP 10

说明：图中的红颜色字体

图中黑颜色字体要求发

```
R1(config-router)# network 10.0.0.0
R1(config-router)# no auto-summary
R1(config-router)# exit
R1(config)# access-list 100 permit gre host 12.0.0.1 host 23.0.0.2
```

R2 路由器命令配置:

```
R2(config)# interface Serial0/0
R2(config-if)# ip address 12.0.0.2 255.255.255.252
R2(config)# interface Serial0/1
R2(config-if)# ip address 23.0.0.1 255.255.255.252
R2(config)# router eigrp 10
R2(config-router)# network 23.0.0.0
R2(config-router)# network 12.0.0.0
R2(config-router)# no auto-summary
R2(config-router)# end
```

R3 路由器命令配置

```
R3(config)# crypto isakmp policy 2
R3(config-isakmp)# encr 3des
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
```

```
R3(config)# crypto isakmp key cisco address 12.0.0.1
R3(config)# crypto ipsec transform-set TEST000 esp-3des esp-md5-hmac
R3(config)# crypto map R3 1 ipsec-isakmp
R3(config-crypto-map)# set peer 12.0.0.1
R3(config-crypto-map)# set transform-set TEST000
R3(config-crypto-map)# match address 100
```

```
R3(config)# interface Loopback0
R3(config-if)# ip address 3.3.3.3 255.255.255.255
R3(config)# interface Tunnel0
R3(config-if)# ip address 10.0.0.2 255.255.255.252
R3(config-if)# tunnel source Serial0/1
R3(config-if)# tunnel destination 12.0.0.1
R3(config-if)# crypto map R3
R3(config)# interface Serial0/1
R3(config-if)# ip address 23.0.0.2 255.255.255.252
R3(config-if)# crypto map R3
R3(config)# interface FastEthernet1/0
R3(config-if)# ip address 192.168.3.92 255.255.255.0 //用于连接 PC 机，可使用 SDM 配置
```

```
R3(config)# router eigrp 10
R3(config-router)# network 23.0.0.0
R3(config-router)# no auto-summary
```

```
R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# network 3.0.0.0
R3(config-router)# network 10.0.0.0
R3(config-router)# no auto-summary
R3(config)# access-list 100 permit gre host 23.0.0.2 host 12.0.0.1
```

以上配置完成。

测试方法：

查看 ACL 能够检测到有匹配的数据包被加密

```
R3#show ip access-lists
```

Extended IP access list 100

```
10 permit gre host 23.0.0.2 host 12.0.0.1 (142 matches)
```

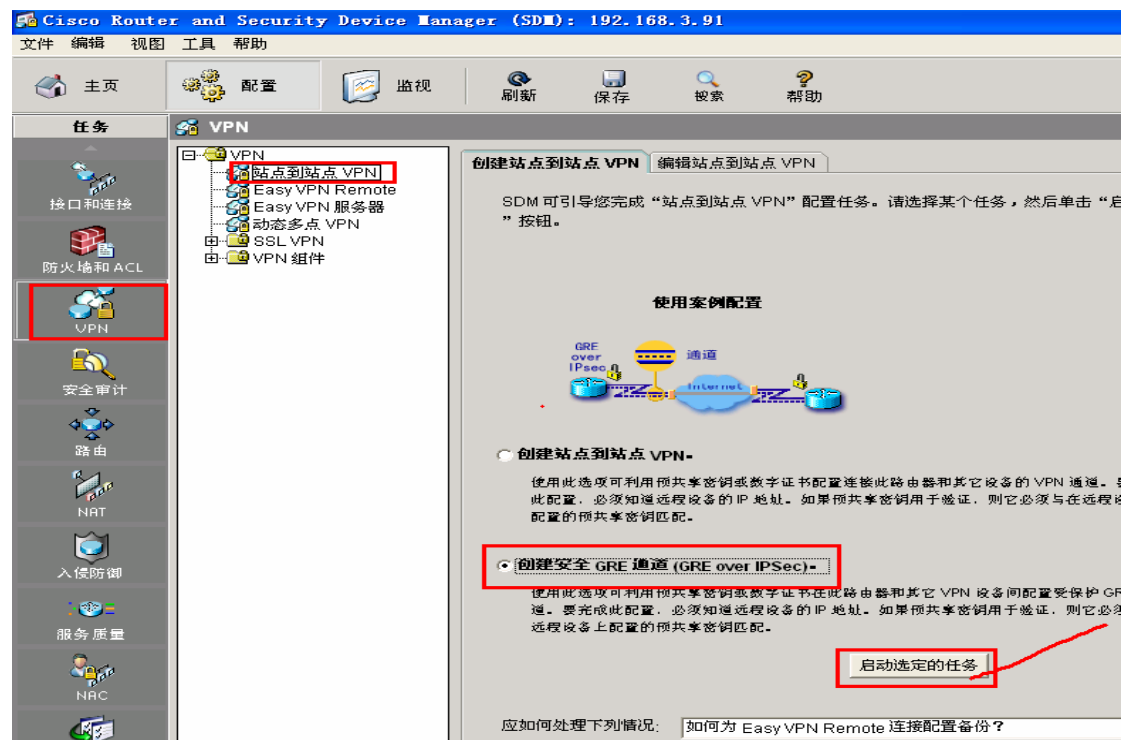
显示：当前已经有 142 个数据包被匹配加密

使用 SDM 完成配置步骤：

第 1 步 点击 VPN



第 2 步 点击“创建安全的 GRE 通道”选项



第 3 步 下一步继续



第 4 步 设定 Tunnel 信息



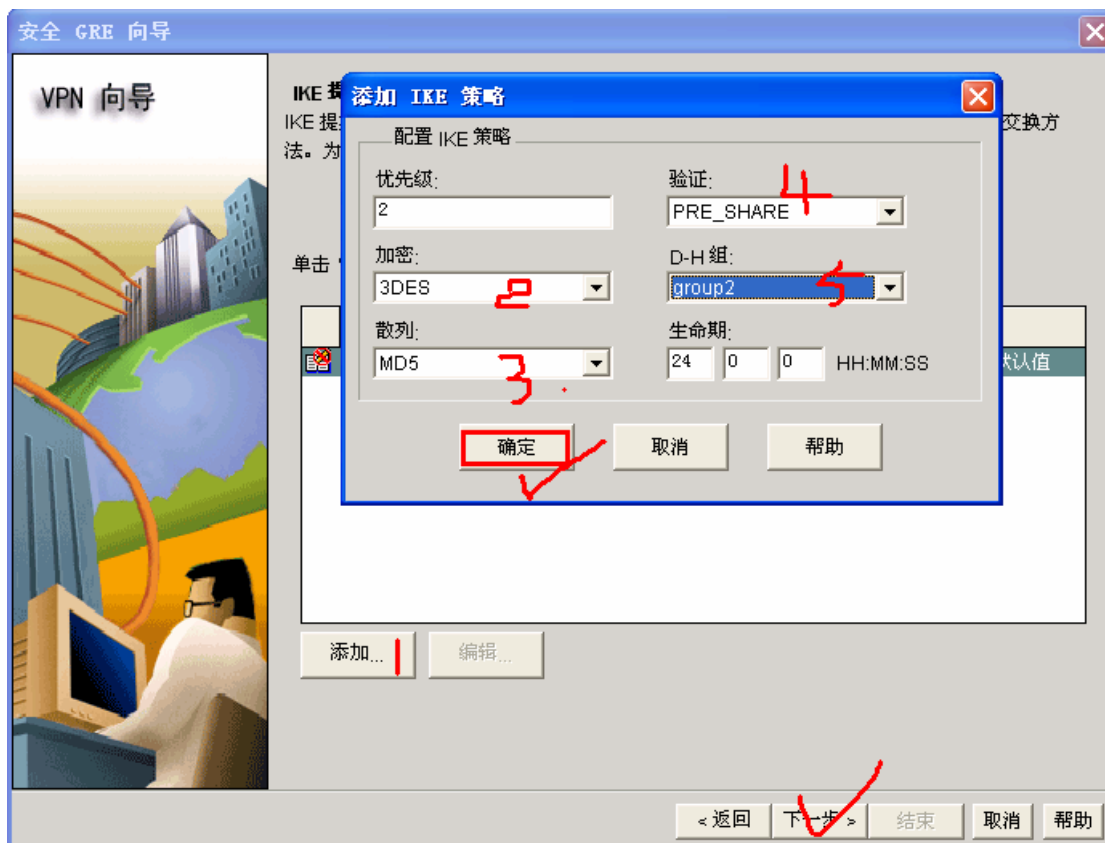
第 5 步 忽略，继续下一步



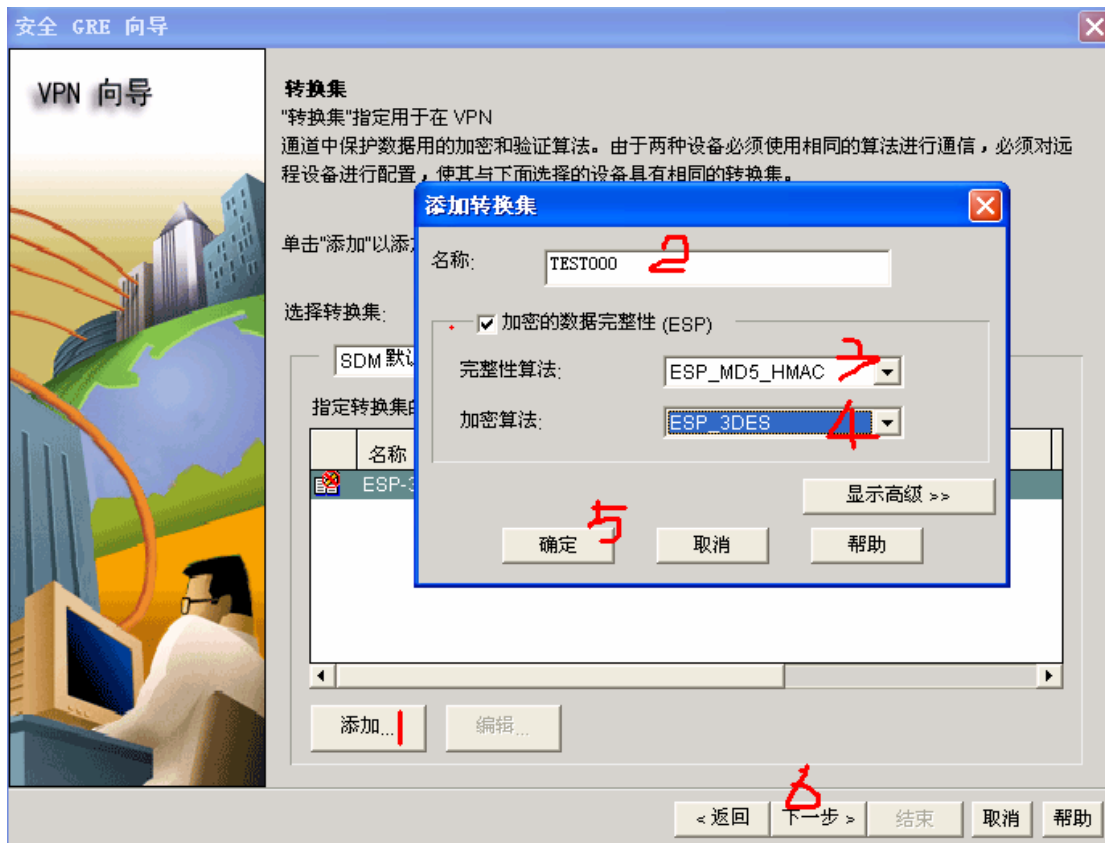
第 6 步 设定预共享密钥为 cisco



第 7 步 设定 IKE 的策略



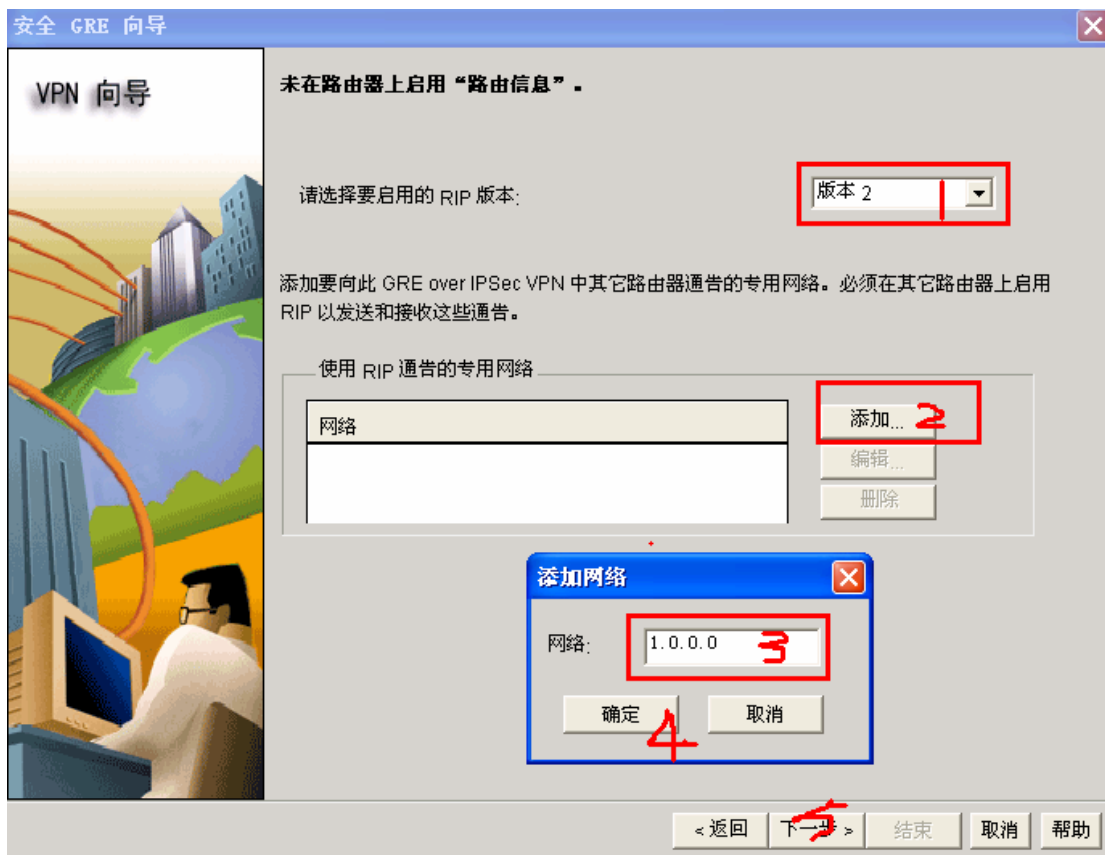
第 8 步 配置转换集



第 9 步 选定应用于 GRE 通道的路由协议为 RIPv2



第 10 步 将私网路由发布 RIPv2 路由协议中



第 11 步 配置完成



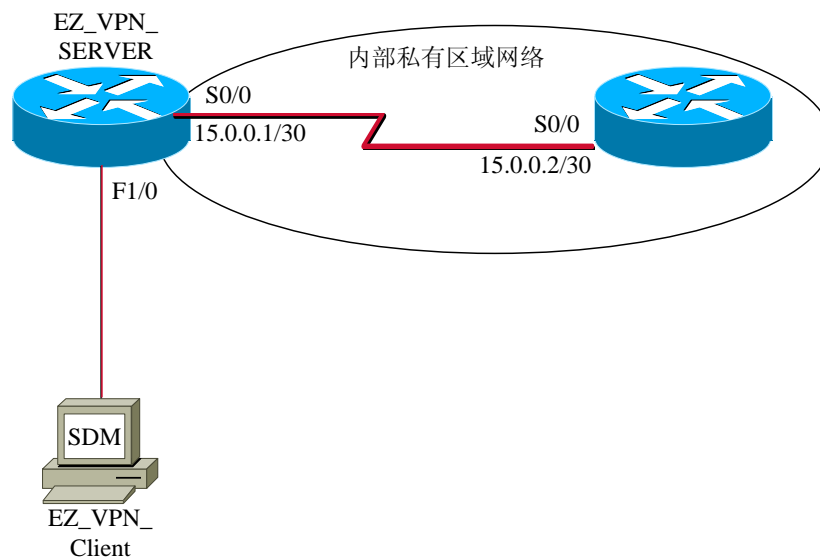
3.6. Cisco Easy VPN

3.6.1. 组成部分

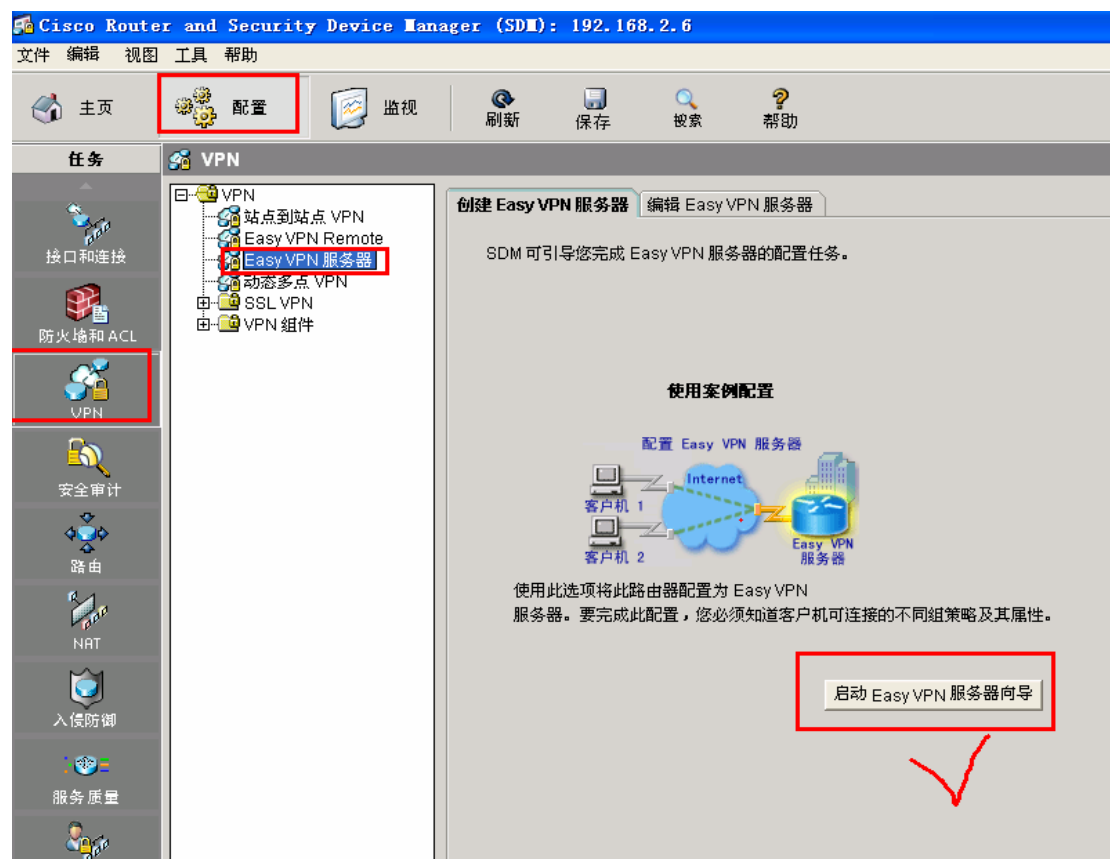
- Easy VPN Server: 使用路由器、防火墙等配置 Server 端
- Easy VPN Client: 一般使用 PC 电脑通过客户端工具进行连接

3.6.2. 前期配置步骤

- 配置系统用户名和密码，可以是 1 级用户
Router(config)# username ccnp password ccnp
- 配置 enable 特权密码
Router(config)# enable password cisco
- 启用 AAA 使用本地数据库认证
Router(config)# aaa new-model
Router(config)# aaa authentication login default local
- 使用 SDM 工具配置 VPN Server 向导



第 1 步 选择启用建立 Easy VPN Server 操作向导



第 2 步 点击下一步开始操作



第 3 步 选择作 Easy VPN Server 的连接接口，和用户验证方式

Easy VPN 服务器向导 - 10% 已完成

VPN 向导

接口和验证

接口

请选择应在其上配置 Easy VPN 服务器的接口。Easy VPN 客户机将通过此接口连接到服务器。

此 Easy VPN 服务器的接口：

FastEthernet1/0

选择一项

FastEthernet1/0

验证

选择验证 VPN 客户机（连接至此 Easy VPN 服务器）的方法。

☒ 预共享密钥 ☐ 数字证书 ☐ 两者

您可选取一个参与站点到站点 VPN 连接的接口。但如接口参与的是 GRE over IPSec、DMVPN 或 Easy VPN 客户机连接，则不能选取该接口。

有关详细信息，请单击帮助按钮。

Internet

< 返回 下一步 > 结束 取消 帮助

第 4 步 配置 IKE 的策略

Easy VPN 服务器向导 - 20% 已完成

VPN 向导

添加 IKE 策略

配置 IKE 策略

优先级: 2

加密: 3DES

散列: MD5

验证: PRE_SHARE

D-H 组: group2

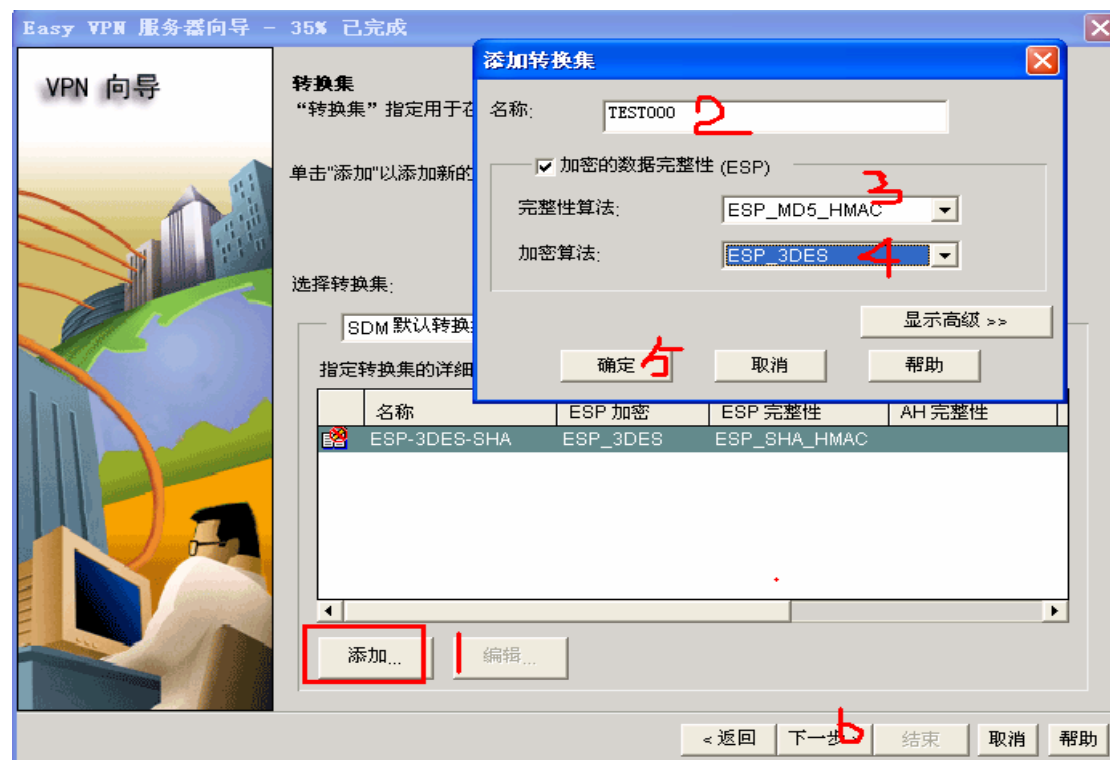
生命期: 24 0 0 HH:MM:SS

确定 取消 帮助

添加... 编辑...

< 返回 下一步 > 结束 取消 帮助

第 5 步 设定转换集(transform set)



第 6 步 选择 VPN 客户端用户连接的验证方式



第 7 步 选择第 2 验证方式，同时可填加设备本地用户的帐号



Easy VPN 服务器向导 - 65% 已完成

VPN 向导

用户验证[扩展验证]

用户验证 (扩展验证) 验证经 IKE 验证的设备用户以提供其它安全性。用户凭证扩展验证可以在此路由器和/或外部服务器上本地配置。

☒ 启用用户验证

选择将用于配置用户凭证的服务器，或选择一个现有 AAA 策略，它定义了用于配置用户凭证的服务器。

☒ 仅限本地

☐ 仅限 RADIUS 和本地

☐ 选择现有 AAA 方法列表

添加 RADIUS 服务器...

选择一项

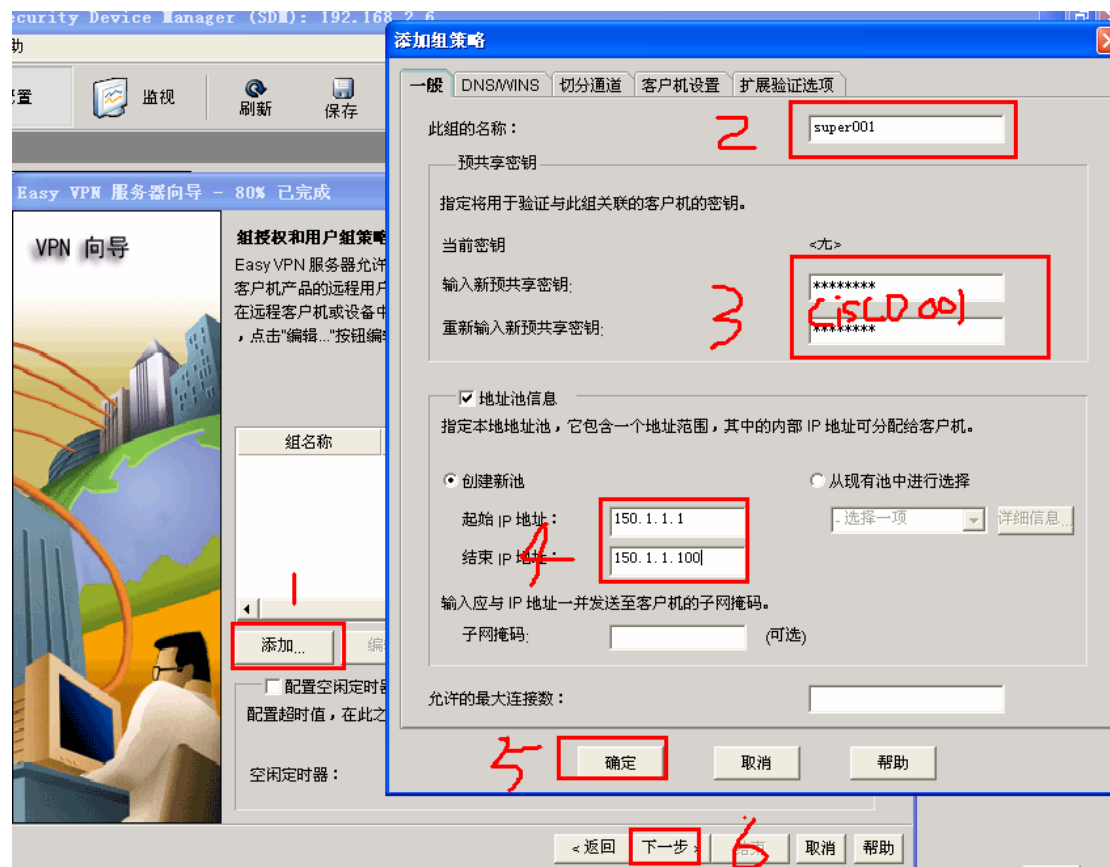
添加用户凭证...

摘要

将使用本地数据库进行用户验证。

< 返回 下一步 > 结束 取消 帮助

第 8 步 添加 VPN 客户端的用户名和密码



Security Device Manager (SDM): 192.168.2.6

配置 监视 刷新 保存

Easy VPN 服务器向导 - 80% 已完成

VPN 向导

组授权和用户组策略

Easy VPN 服务器允许客户机产品的远程用户在远程客户机或设备中，点击“编辑...”按钮编辑。

组名称

添加...

配置空闲定时器：配置超时值，在此之后空闲定时器：

添加组策略

一般 DNS/MINS 切分通道 客户机设置 扩展验证选项

此组的名称：2 super001

预共享密钥

指定将用于验证与此组关联的客户机的密钥。

当前密钥 <无>

输入新预共享密钥：3 *****

重新输入新预共享密钥：(isLD 00) *****

☒ 地址池信息

指定本地地址池，它包含一个地址范围，其中的内部 IP 地址可分配给客户机。

☒ 创建新池

☐ 从现有池中进行选择

起始 IP 地址：150.1.1.1

结束 IP 地址：150.1.1.100

输入应与 IP 地址一并发送至客户机的子网掩码。

子网掩码：(可选)

允许的最大连接数：

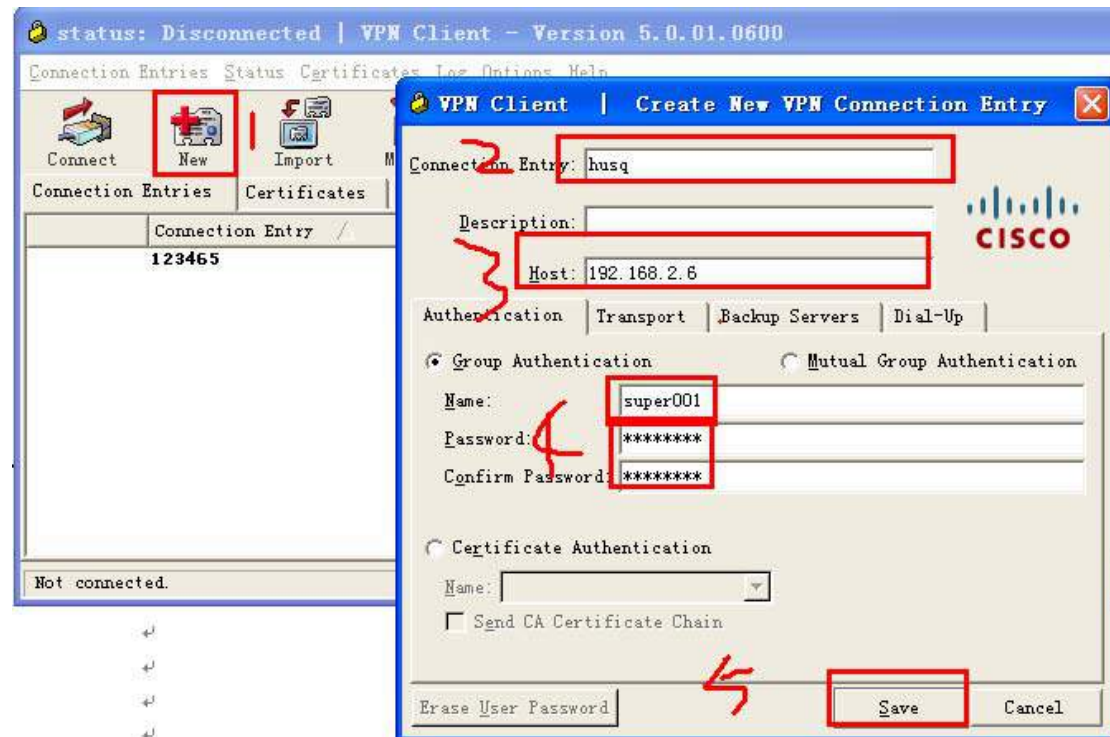
5 确定 取消 帮助

< 返回 下一步 > 取消 帮助

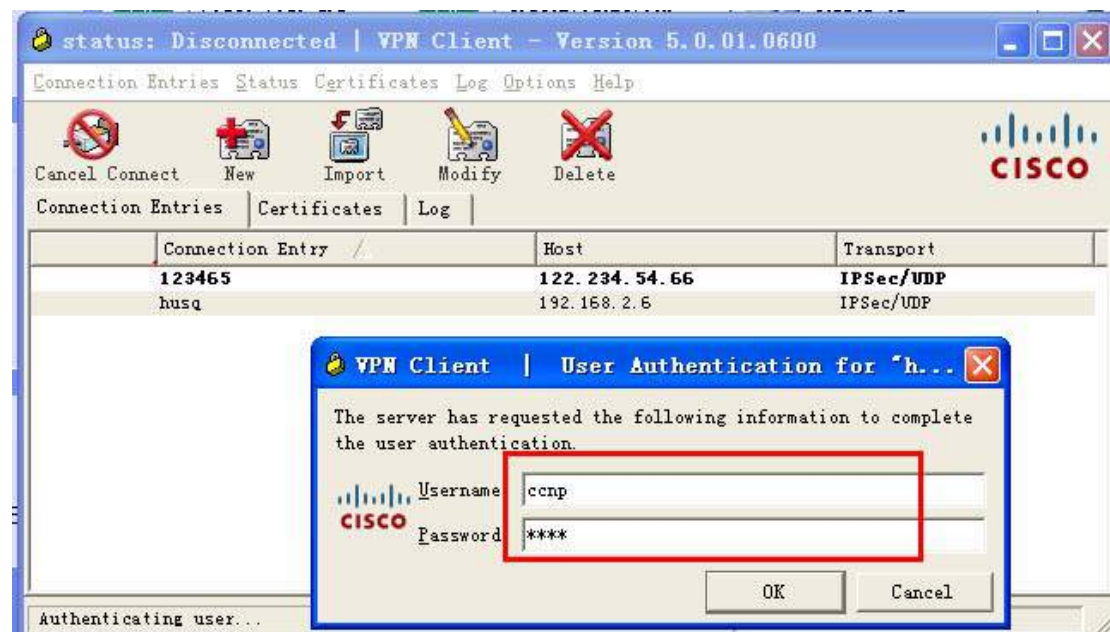
第 9 步 完成配置



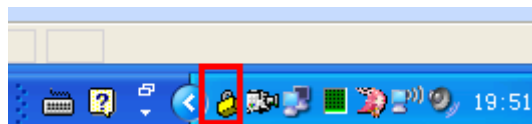
第 10 步 使用 VPN 客户端进行连接测试，输入组名和预共享密钥：



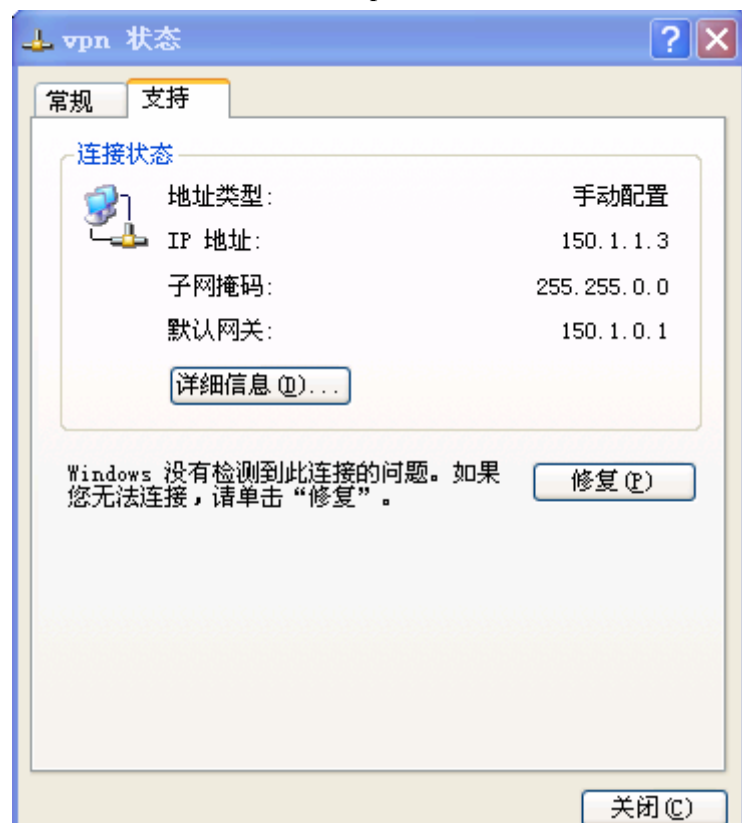
第 11 步 开始点击连接 Connect 按钮，会提示输入路由器上配置的用户名和密码



若连接成功，可在状态栏图标显示 小锁已经锁住了



可查看网络连接选项里面的 vpn 连接状态。可以查看出获得的地址



特别说明： 如果使用模拟器做此实验，在本机上使用 vpn 客户端工具拨入到模拟器后，本机不能够直接访问 VPN 的私网地址。不过，可以使用其它机器拨入，立即可以访问。

Easy VPN 的命令行模式配置

```
Server(config)# enable secret cisco
Server(config)# username super privilege 15 password 0 cisco123 （创建超级用户）
Server(config)# username ccnp password ccnp (创建 1 级权限用户，为连接 SDM 定义的用户)
Server(config)# crypto isakmp policy 1
Server(config-isakmp)# encr 3des
Server(config-isakmp)# authentication pre-share
Server(config-isakmp)# hash md5
Server(config-isakmp)# group 2
```

```
Server(config)# crypto isakmp client configuration group super001 //vpn 客户端登陆帐号
Server(config-isakmp-group)# key cisco001 //vpn 客户端登陆密码
Server(config-isakmp-group)# pool ADD //vpn 客户端地址池
Server(config-isakmp-group)# acl 150 //调用 ACL 150，启用隧道分离
Server(config-isakmp-group)# end
```

```
Server(config)# crypto ipsec transform-set TEST000 esp-3des esp-md5-hmac
Server(config)# crypto dynamic-map TEST-MAP 1
Server(config-crypto-map)# set transform-set TEST000
Server(config-crypto-map)# reverse-route //逆向路由
Server(config-crypto-map)# exit
```

```
Server(config)# crypto map VPNMAP isakmp authorization list super001
Server(config)# crypto map VPNMAP client configuration address respond
Server(config)# crypto map VPNMAP 1 ipsec-isakmp dynamic TEST-MAP
```

```
Server(config)# interface FastEthernet1/0
Server(config-if)# ip address 192.168.2.6 255.255.255.0
Server(config-if)# crypto map VPNMAP
Server(config)# interface Serial0/0
Server(config-if)# ip address 12.0.0.1 255.255.255.252
```

```
Server(config)# access-list 150 permit ip 192.168.2.0 0.0.0.255 any
Server(config)# ip local pool ADD 150.1.1.1 150.1.1.200 //为 VPN 客户端创建地址池
```

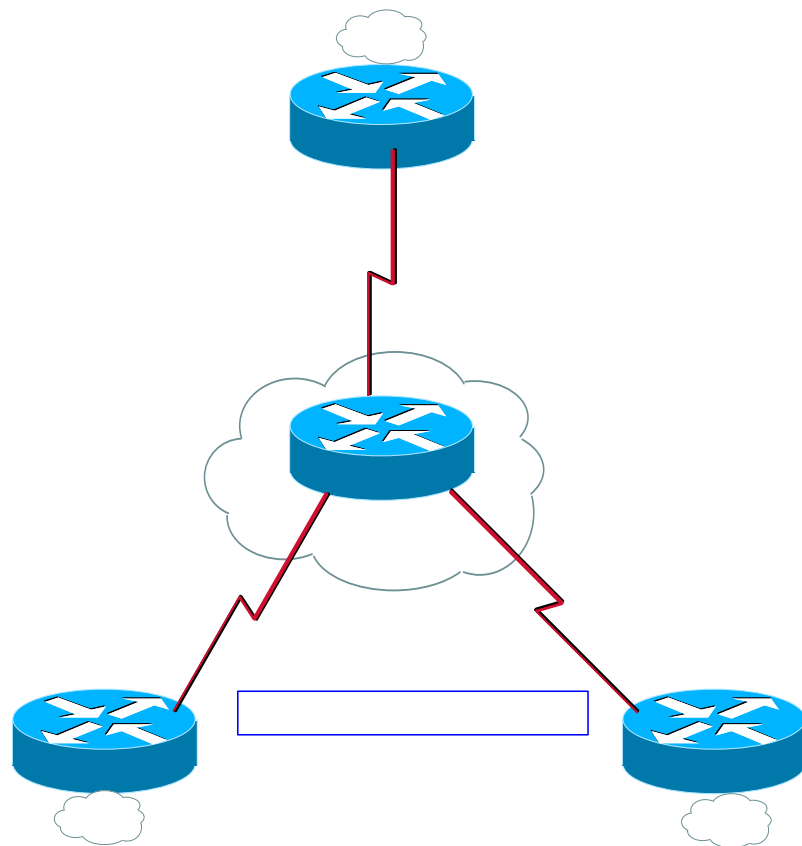
```
Server(config)# line vty 0 4
Server(config-line)# privilege level 15
Server(config-line)# login local
Server(config-line)# transport input telnet ssh
```

3.7.DMVPN动态多点VPN

3.7.1. DMVPN的特性:

- 1、站点 VPN 的客户端的 IP 允许是动态的
- 2、VPN Server 端要求是固定 IP 地址

3.7.2. 实验拓扑图

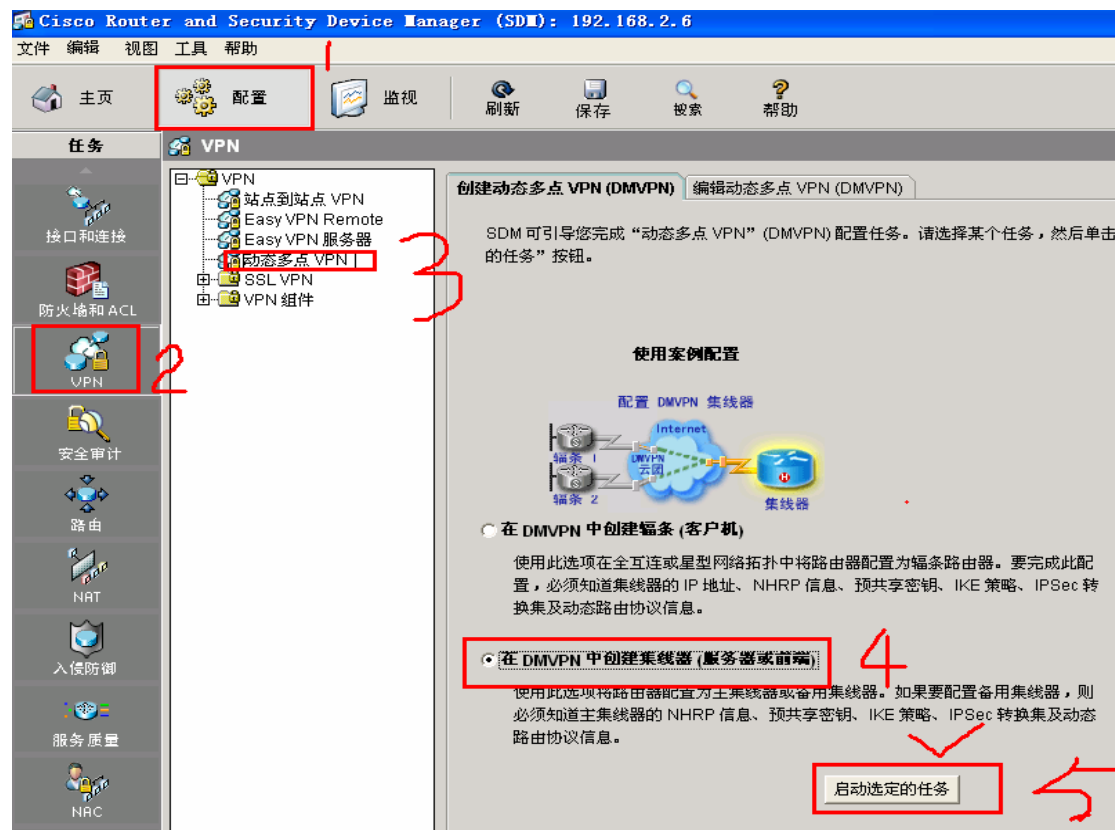


L0:1.

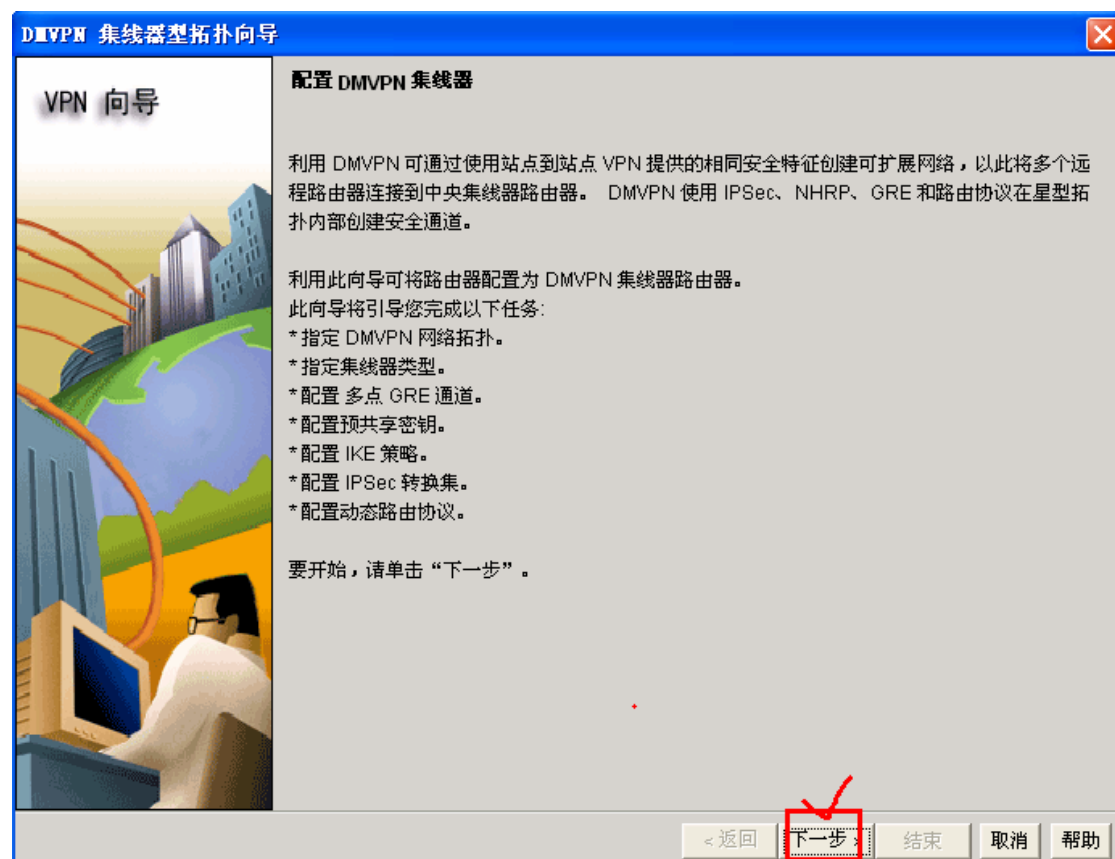
Tunnel0:
10.0.0.1/24
EIGRP 10

配置 DMVPN 的**服务端**:

第 1 步 点击动态多点 VPN 选项, 并启动选定的任务



第 2 步 开始进入服务端配置向导



第3步 选定“全互联结构”

DMVPN 集线器型拓扑向导 - 已完成 10%

VPN 向导

DMVPN 网络拓扑
选择 DMVPN 网络拓扑。

☐ 星型网络

在此拓扑中，所有 DMVPN 通信均通过集线器路由发送。在辐条路由器上将配置点到点（P2P）接口，并且该辐条路由器将用其创建连接活动集线器的通道。这些辐条路由器将不创建与拓扑中其它辐条路由器相连的 GRE 通道。

☒ **全互联网络**

在此拓扑中，该辐条设备将动态建立连接其它辐条设备的直接通道，并将直接向其发送 DMVPN 通信。将在该辐条设备上配置多点 GRE 通道接口以支持此功能。

注意: Cisco 仅在以下 Cisco IOS 映像中支持全互联 DMVPN 网络: 12.3(8)T1 和 12.3(9) 或更高版本。

全互联网络



第4步 选定：主集线器

DMVPN 集线器型拓扑向导 (全互联拓扑) - 已完成 15%

VPN 向导

集线器类型
在 DMVPN 网络中，应存一个集线器型路由器和多个与其相连的辐条型路由器。您还可将路由器配置为集线器。而将其它路由器作为备用集线器。请选择要将此路由器配置成何种集线器。

☒ **主集线器**

☐ 备用集线器

第 5 步 配置 GRE 通道，并设定 NHRP(下一跳路由协议)的默认值

DMVPN 集线器型拓扑向导 (全互连拓扑) - 已完成 40%

VPN 向导

验证

选择要用于为 DMVPN 网络中的对等项验证此路由器的方法。可使用数字证书或预共享密钥。如使用数字证书，则路由器必须配置有效的证书。如果使用预共享密钥，则此路由器上配置的密钥须与 DMVPN 网络中所有其它路由器上配置的密钥匹配。

☐ 数字证书

☒ **预共享密钥**

预共享密钥: *****

重新输入密钥: *****

GISCD

< 返回 **下一步 >** 结束 取消 帮助

第 6 步 采用默认的 IKE 策略

DMVPN 集线器型拓扑向导 (全互连拓扑) - 已完成 50%

VPN 向导

IKE 提案

IKE 提案指定与远程设备协商 VPN 连接时此路由器使用的加密算法、验证算法和密钥交换方法。为与远程设备建立 VPN 连接，必须至少通过下面列出的策略之一配置远程设备。

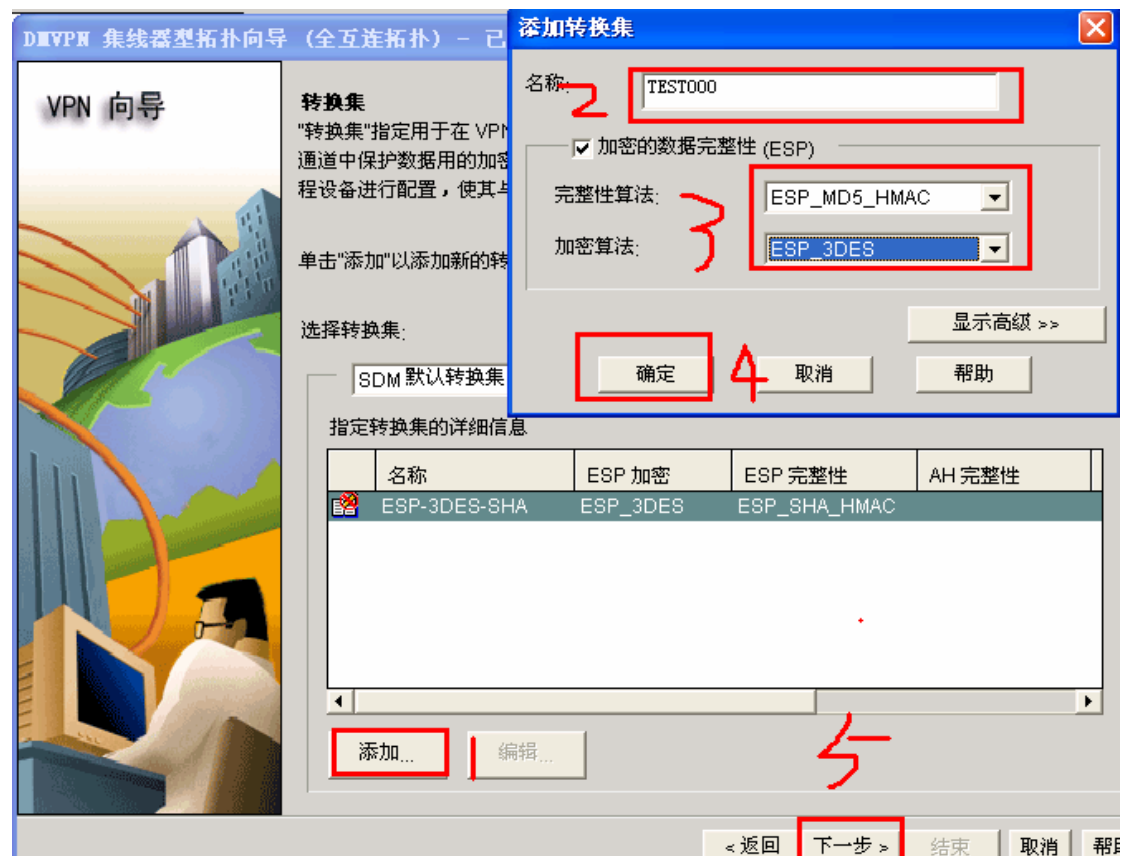
单击“添加...”按钮添加更多策略，单击“编辑...”按钮编辑现有策略。

	优先级	加密	散列	D-H 组	验证	类型
1	3DES	SHA_1	group2	PRE_SHARE	SDM 默认值	

添加... 编辑...

< 返回 **下一步 >** 结束 取消 帮助

第 7 步 设定转换集属性



第 8 步 选择应用 Tunnel 接口的内部路由协议



第 9 步 配置应用于在私网传输中的路由协议 eigrp 10

DMVPN 集线器型拓扑向导 (全互连拓扑) - 已完成 80%

VPN 向导

未在路由器上启用“路由信息”。

☐ 选择现有 EIGRP AS 号:
☒ 新建 EIGRP AS 号:

添加要在此 DMVPN 中其它路由器通告的专用网络。此 DMVPN 中的其它路由器必须在同一自治系统中。

使用 EIGRP 通告的专用网络

网络	通配符掩码

添加...

编辑...

删除...

将向 DMVPN 云团通告的专用网络。

Internet

DMVPN 云团

添加网络

网络: 1.0.0.0

通配符掩码:

确定 取消

< 返回 下一步 > 结束 取消 帮助

第 10 步 结束配置

DMVPN 集线器型拓扑向导 (全互连拓扑) - 已完成 90%

VPN 向导

配置汇总

单击“完成”，将配置传送到您的路由器。

此路由器的角色: DMVPN集线器 (主要)
将此路由器连接到 Internet 的接口: Serial0/0
此路由器通道接口的 IP 地址: 10.0.0.1 掩码 255.255.255.0
通道接口的高级配置:
NHRP 验证字符串: DMVPN_NW
NHRP 网络 ID: 100,000
NHRP 持有时间: 360
通道密钥: 100,000
带宽: 1,000
MTU: 1,400
延迟: 1,000
路由协议: EIGRP
EIGRP 自治系统编号: 10
已通告的专用网络:
1.0.0.0
转换集:
名称: TEST000
ESP 加密: ESP_3DES
ESP 完整性: ESP_MD5_HMAC
模式: TUNNEL
IKE 策略:

辐条配置...

< 返回 下一步 > 结束 取消 帮助

配置 DMVPN 的客户端

第 1 步 选定配置 DMVPN 的客户端选项

Cisco Router and Security Device Manager (SDM): 192.168.2.7

文件 编辑 视图 工具 帮助

主页 配置 监视 刷新 保存 搜索 帮助

任务

VPN

- VPN
 - 站点到站点 VPN
 - Easy VPN Remote
 - Easy VPN 服务器
 - 动态多点 VPN
 - SSL VPN
 - VPN 组件

接口和连接

防火墙和 ACL

VPN

安全审计

路由

NAT

入侵防御

服务质量

NAC

创建动态多点 VPN (DMVPN) 编辑动态多点 VPN (DMVPN)

SDM 可引导您完成“动态多点 VPN” (DMVPN) 配置任务。请选择某个任务，然后单击“任务”按钮。

使用案例配置

配置 DMVPN 辐条

辐条 1

Internet

DMVPN 云团

集线器

☒ 在 DMVPN 中创建辐条 (客户端)

使用此选项在全互连或星型网络拓扑中将路由器配置为辐条路由器。要完成此配置，必须知道集线器的 IP 地址、NHRP 信息、预共享密钥、IKE 策略、IPSec 转换集及动态路由协议信息。

☐ 在 DMVPN 中创建集线器 (服务器或前端)

使用此选项将路由器配置为主集线器或备用集线器。如果要配置备用集线器，必须知道主集线器的 NHRP 信息、预共享密钥、IKE 策略、IPSec 转换集及动态路由协议信息。

启动选定的任务

第 2 步 进入客户端配置向导

DMVPN 辐条型拓扑向导

VPN 向导

配置 DMVPN 辐条拓扑

利用 DMVPN 可通过使用站点到站点 VPN 提供的相同安全特征创建可扩展网络，以此将多个远程路由器连接到中央集线器路由器。DMVPN 使用 IPSec、NHRP、GRE 和路由协议在星型拓扑内部创建安全通道。

利用此向导可将路由器配置为 DMVPN 辐条路由器。

此向导将引导您完成以下任务：

- * 指定 DMVPN 网络拓扑。
- * 提供集线器信息。
- * 配置 GRE 通道接口。
- * 配置预共享密钥。
- * 配置 IKE 策略。
- * 配置 IPSec 转换集。
- * 配置动态路由协议。

要开始，请单击“下一步”。

< 返回 下一步 > 结束 取消 帮助

第 3 步 选择全互联结构

DMVPN 辐条型拓扑向导 - 已完成 10%

VPN 向导

DMVPN 网络拓扑
选择 DMVPN 网络拓扑。

☐ 星型网络

在此拓扑中，所有 DMVPN 通信均通过集线器路由发送。在辐条路由器上将配置点到点接口，并且该辐条路由器将用其创建连接活动集线器的通道。这些辐条路由器将不创建拓扑中其它辐条路由器相连的 GRE 通道。

☒ **全互联网络**

在此拓扑中，该辐条设备将动态建立连接其它辐条设备的直接通道，并将直接向其发送 DMVPN 通信。将在该辐条设备上配置多点 GRE 通道接口以支持此功能。

注意:Cisco 仅在以下 Cisco ISO 映像中支持全互联 DMVPN 网络:12.3(8)T1 和 12.3(9) 或更高版本。



全互联网络

辐条 Internet 集线器 DMVPN 云团

< 返回 **下一步 >** 结束 取消

第 4 步 配置连接 DMVPN 服务端的地址信息(固定物理地址与隧道接口地址)

DMVPN 辐条型拓扑向导 (全互联拓扑) - 已完成 20%

VPN 向导

指定集线器信息
输入集线器的 IP 地址及集线器中加入此 DMVPN 网络的多点 GRE 通道接口的 IP 地址。请联系您的网络管理员获取此信息。您可指定备用集线器，以便主集线器出现故障时进行替换。

集线器信息

集线器物理接口的 IP 地址:
12.0.0.1

集线器 mGRE 通道接口的 IP 地址:
10.0.0.1

☐ 备用集线器

集线器物理接口的 IP 地址:
集线器 mGRE 通道接口的 IP 地址:



要在以上输入的公共 IP 地址

要在以上输入的 mGRE 通道 IP 地址

主集线器 备用集线器

您正在配置此辐条路由器

< 返回 **下一步 >** 结束 取消

第 5 步 设定 GRE 的通道接口信息，同时使用默认的 NHRP 设置

DMVPN 辐条型拓扑向导 (全互连拓扑) - 已完成 30%

VPN 向导

多点 GRE 通道接口配置

选择连接到 Internet 的接口: Serial0/0

为拨号连接选择配置的接口可能会使连接始终处于启用状态。

多点 GRE (mGRE) 通道接口

为此 DMVPN 连接创建 GRE 通道接口。请输入此接口的地址信息。

通道接口的 IP 地址

IP 地址: 10.0.0.3

子网掩码: 255.255.255.0 24

高级设置

单击“高级”以验证值与对等项设置是否匹配。

高级...

通道接口的高级配置

在此 DMVPN 的所有设备中，以下参数中的某些参数应相同。更改 SDM 默认值前，请从网络管理员那里获取正确值。

NHRP

NHRP 验证字符串: DMVPN_NW

NHRP 网络 ID: 100000

NHRP 持有时间: 360

GRE 通道接口信息

通道密钥: 100000

带宽: 1000

MTU: 1400

通道吞吐延迟: 1000

确定 取消 帮助

Internet

DMVPN 云团

逻辑 GRE/mGRE 通道接口。所有集线器和端路由器上 GRE/mGRE 通道接口的 IP 地址均属私有 IP 地址。它们必须位于同一子网内。有关详细信息，请单击帮助按钮。

< 返回 下一步 > 结束 取消

第 6 步 设置预共享密钥为：cisco

DMVPN 辐条型拓扑向导 (全互连拓扑) - 已完成 40%

VPN 向导

验证

选择要用于为 DMVPN 网络中的对等项验证此路由器的方法。可使用数字证书或预共享密钥。使用数字证书，则路由器必须配置有效的证书。如果使用预共享密钥，则此路由器上配置的密钥须与 DMVPN 网络中所有其它路由器上配置的密钥匹配。

☐ 数字证书

☒ 预共享密钥

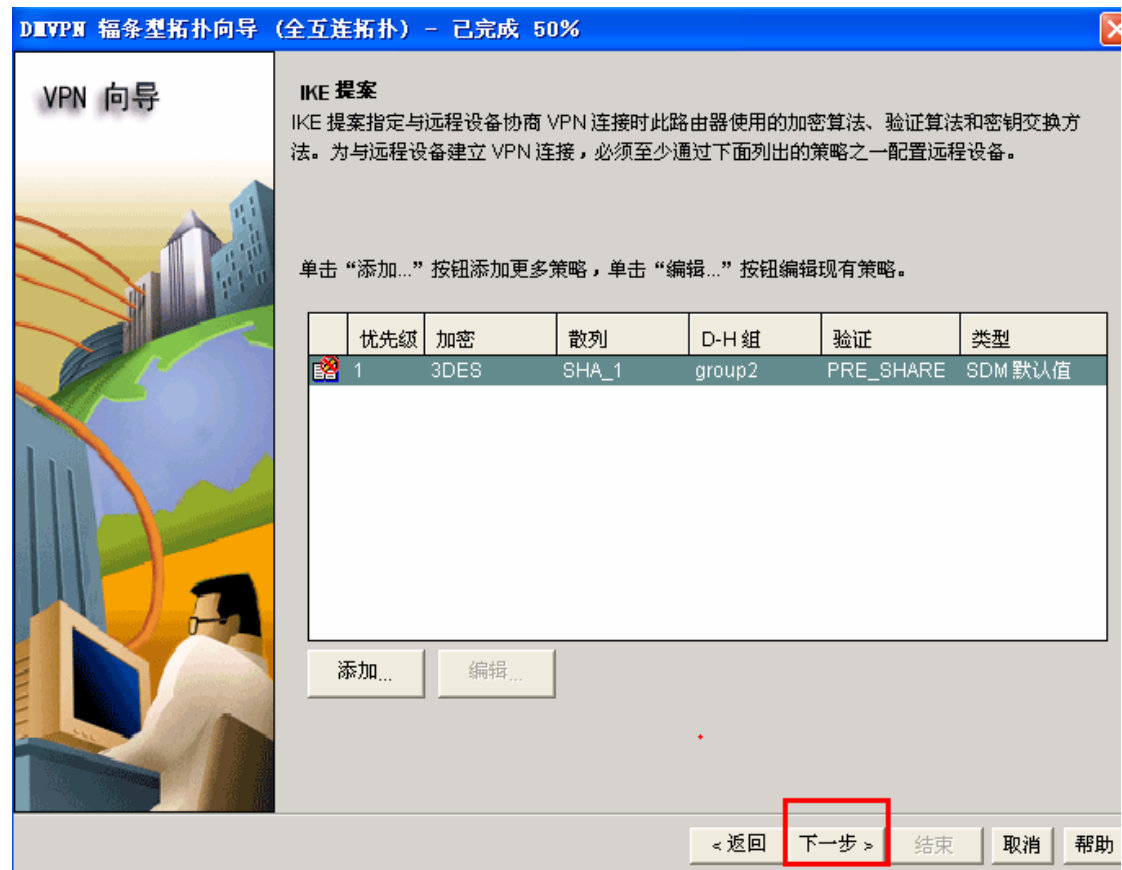
预共享密钥: *****

重新输入密钥: *****

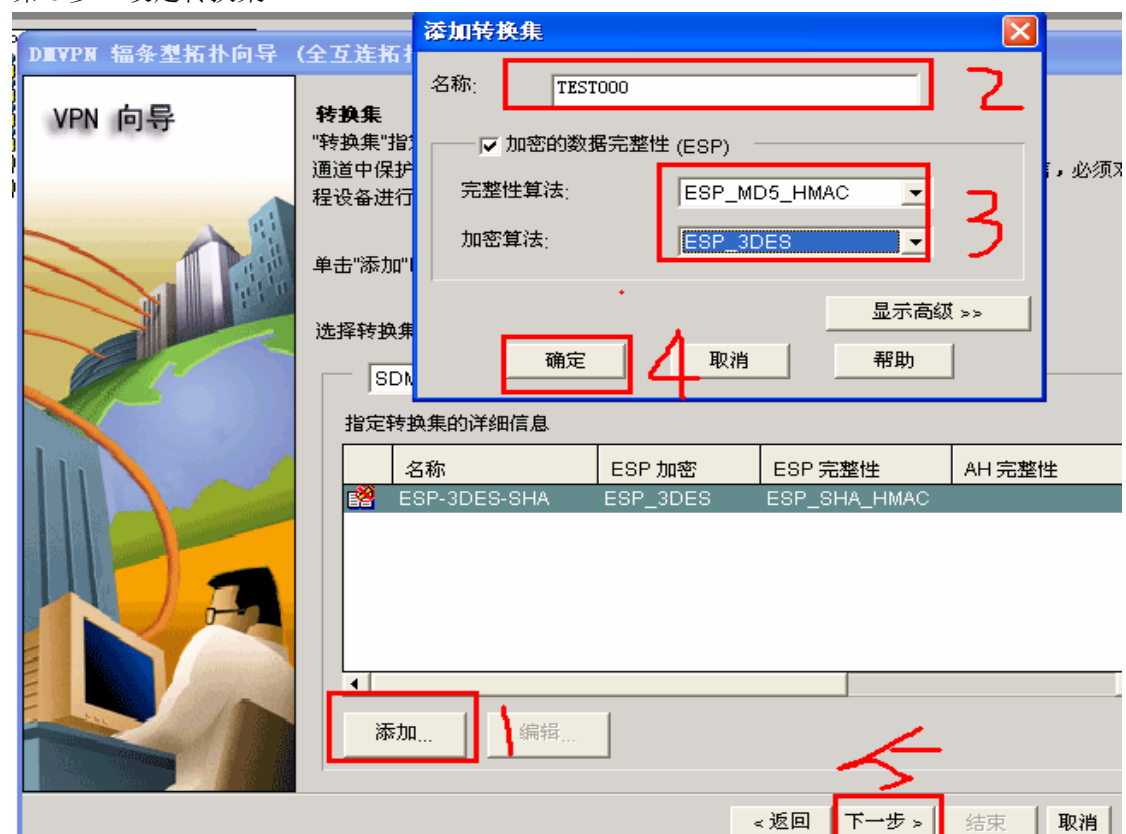
cisco

< 返回 下一步 > 结束 取消

第 7 步 采用默认的 IKE 策略



第 8 步 设定转换集



第 9 步 启用应用于私网内的路由协议 eigrp 10



第 10 步 配置 EIGRP 信息



第 11 步 结束配置



3.8. 启用SSH进行远程登陆

3.8.1. 启用SSH进行远程登陆

```
Router(config)# username super001 privilege 15 password cisco001
```

```
Router(config)# ip domain name test //配置 domain 名称
```

```
Router(config)# crypto key generate rsa
```

```
Router(config)# line vty 0 15
```

```
Router(config-line)# login local
```

```
Router(config-line)# transport input ssh telnet //两种都支持
```

4. CCNP ONT 课程

4.1. QOS(服务质量保证)

4.1.1. QoS的概念:

QoS被称为：服务质量保证。QoS的机制是为了给重要的业务提供一个可靠的数据传输，给予重要业务的带宽和延迟的保证。如果网络的带宽非常充裕的情况下，QoS将是毫作用的。

4.1.2. QoS的服务模型

Best-Effort service 尽力而为的服务模型

Integrated service 综合服务模型(或称为集成的服务模型) 简称**Intserv**

Differentiated service 区分服务模型 简称**Diffserv**

➤ 尽力而为的服务模型

数据有什么传什么，阻塞了就阻塞了，丢弃就丢弃了，不会任何数据做流量控制。这种服务模型也是Internet 的缺省服务模型。

➤ 综合服务模型

这种服务模型在发送报文前，需要向网络申请特定的服务。应用程序首先通知网络它自己的流量参数和需要的特定服务质量请求：包括带宽、时延等。应用程序一般在收到网络的确认信息，即确认网络已经为这个应用程序的报文预留了资源后，才开始发送报文，同时应用程序发出的报文应该控制在流量参数描述的范围以内。

负责传送QoS请求的信令是RSVP（Resource Reservation Protocol）资源预留协议，它通知路由器应用程序的QoS需求。RSVP是在应用程序开始发送报文之前来为该应用申请网络资源的。

➤ 区分服务模型

根据每个报文指定的QoS 来提供特定的服务 可以用不同的方法来指定报文的QoS，如IP报文的优先级位（IP Precedence），报文的源地址、目的地址、源端口、目的端口、协议号等来区分不同的服务，网络通过这些信息来进行报文的分类、流量整形、流量监管和队列调度。

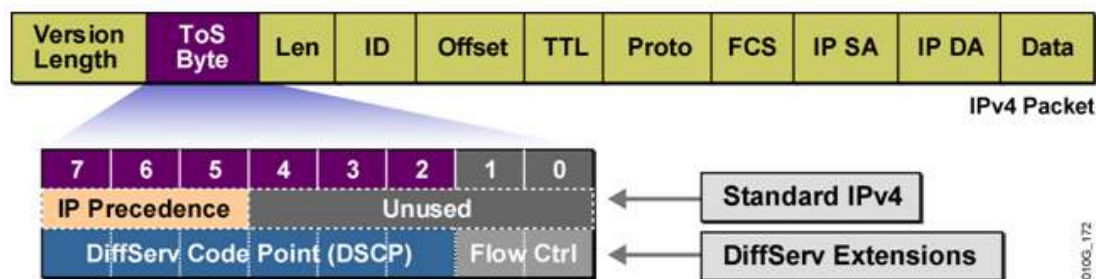
4.1.3. 数据包(ToS)和数据帧(CoS)的分类

DSCP(区分服务代码点)这种标记在frame中和packet中本身就存在，frame中存在CoS字段，packet中有ToS字段

Cos字段：正常的以太网frame中是不存在标记的，但是Dot1q的frame中有三个bit定义服务级别，一共有8个服务级别，其中6个服务级别可以使用。CoS6 和Cos7是预留的。一般可使用的是Cos0-Cos5。Cos5一般被应用于语音。

CoS	Typical Application
7	Reserved
6	Reserved
5	Voice Bearer
4	Video Conferencing
3	Call Signaling
2	High Priority Data
1	Medium Priority Data
0	Best Effort Data

Tos字段：针对于数据包，有两种标识服务类型的方法（如下图所示）分别是IP precedence（ip 优先级）和DSCP（区分服务代码点）



在ip precedence 有8个位用于标识数据包，分别是0—7，7为最高。

DSCP(区分服务代码点)，它使用tos中的前6个位，即DS1-DS5，（如上图所示）定义了0-63一共64个优先级

说明：关于数据包的标识，实际上就是通过更改这些优先级字段将这些数据分出种类来，即便是上面的图标中有所谓的什么0-7优先级，好似7要比0就会优先级大一些，但是一定要清楚这只是区分，执行的策略要靠后面的队列机制来解决，实际上之所以这样定义优先级我认为只是为了制定一个共同遵守的类别优先标准，没有实际的意义，真正的操作是在配置上针对于不同优先级采用的措施——例如在队列里面使用什么标识的数据包属于什么队列等等。

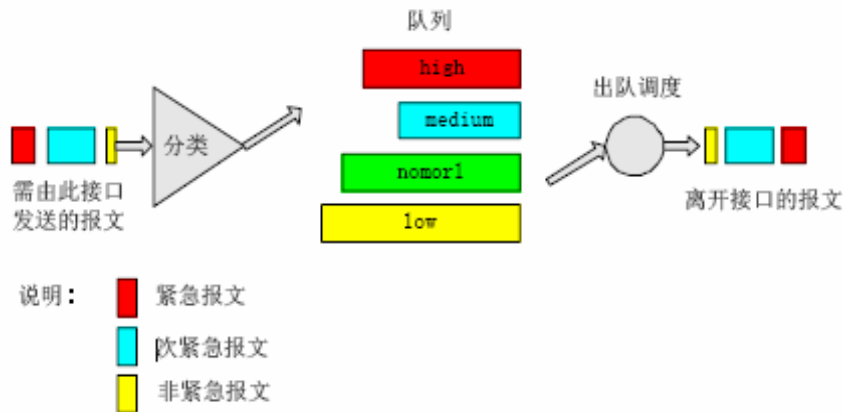
4.1.4. 拥塞管理(队列管理)

QoS使用队列的技术能实现对数据流拥塞管理

队列技术(Queue)：队列技术的原理就是使报文在路由器中按一定的策略暂时缓存到队列中然后再按一定的调度策略把报文从队列中取出，然后再在接口上发送出去。

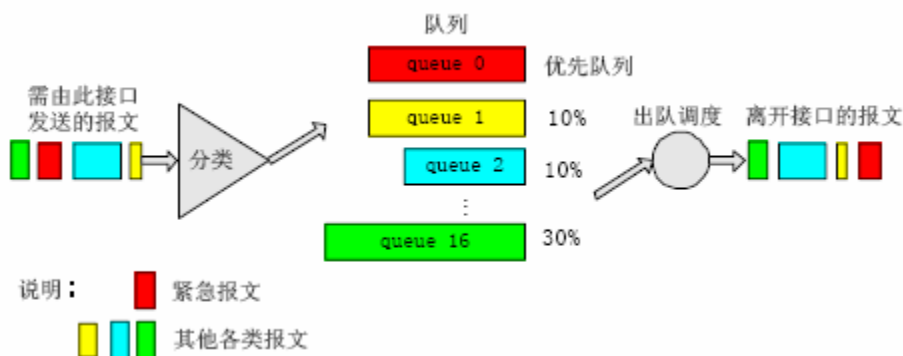
➤ PQ 优先级队列

PQ对报文进行分类，对于IP网络可以根据IP报文的优先级/DSCP等条件进行分类，将所有报文分成最多至4类，分别属于PQ的4个队列中的一个，然后按报文的类别将报文送入相应的队列。PQ的4个队列分别为高优先队列、中优先队列、正常优先队列和低优先队列，它们的优先级依次降低。在报文出队的时候，PQ首先让高优先队列中的报文先出队并发送，直到高优先队列中的报文全部发送完，然后再发送中优先队列中的报文，同样直到发送完后，再正常优先队列和低优先队列的数据。使属于较高优先级队列的报文将会得到优先发送。（下列为：PQ数据包入队及出队图例）



CQ 自定义队列

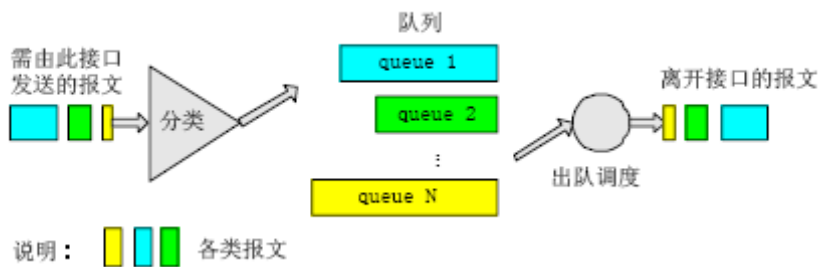
CQ对报文进行分类，报文分成最多16类，分别属于CQ的16个队列中的一个，然后按报文的类别将报文送入相应的队列，实际上队列的号是0-16一共17个，但是0号队列是超级优先队列，路由器总是先把0号队列中的报文发送完然后才处理1到16号队列中的数据包，所以0号队列一般作为系统队列，通常把实时性要求高的交互式协议和链路层协议报文放到0号队列中。1到16号队列可以按用户的定义分配它们能占用接口带宽的比例，在报文出队的时候，CQ按定义的带宽比例分别从1到16号队列中取一定量的报文在接口上发送出去。CQ的自定义队列中1-16号是一个轮循的调度过程。(下列图为CQ的入队和出队队列图)



➤ WFQ(加权公平队列)

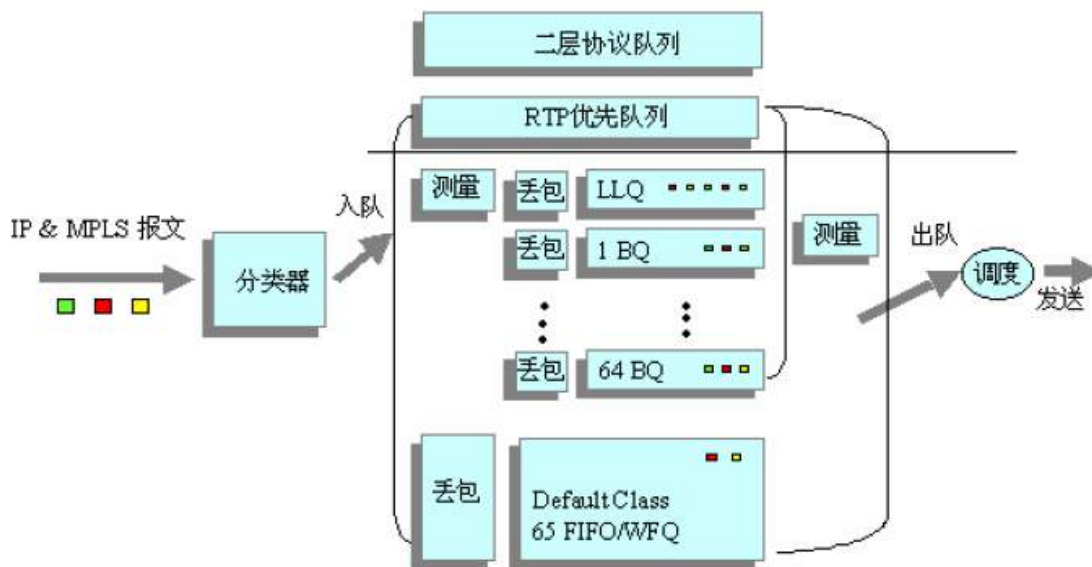
WFQ对报文按流进行分类（对于IP网络相同源IP地址、目的IP地址、源端口号、目的端口号、协议号、IP优先级的报文属于同一个流）每一个流被分配到一个队列，该过程称为散列，采用HASH算法来自动完成。尽量将不同的流分入不同的队列，WFQ的队列数目N可以配置，在出队的时候WFQ按流的IP优先级来分配每个流应占有出口的带宽，优先级的数值越小所得的带宽越少，优先级的数值越大所得的带宽越多，这样就保证了相同优先级业务之间的公平，体现了不同优先级业务之间的权值

注意：WFQ是传输速率低于2.048Mbps的串行接口默认的队列机制。但是WFQ存在一些限制：第一个是WFQ不支持隧道或采用了加密技术的接口，因为这些技术要修改数据包中WFQ用于分类的信息。第二个WFQ提供的带宽控制的精确度不如CBWFQ和CQ等队列机制。(WFQ的入队和出队图例)



➤ CBWFQ(基于类的加权公平队列)

CBWFQ，首先根据IP优先级、DSCP或者输入接口的IP数据流等规则来对报文进行分类，让不同类别的报文进入不同的队列，对于不匹配任何类别的报文将被送入系统定义的缺省类。(下列为CBWFQ应用队列图)



图中所示LLQ（Low Latency Queueing，低延迟队列，后面有）是一个具有较高优先级的队列，它的优先级仅次于二层协议队列（如同CQ中的0号队列），与RTP优先队列（RTP优先队列的参见后文介绍）一个或多个类的报文可以被设定进入LLQ，队列不同类别的报文可设定占用不同的带宽，在调度出队的时候，若LLQ中有报文则总是优先，发送LLQ中的报文直到LLQ中没有报文时或者超过为LLQ配置的最大预留带宽时，才调度发送其他队列中的报文。

4.1.5. 拥塞避免(丢弃策略)

➤ RED 随机早期检测

采用RED时用户可以设定队列的阈值threshold，当队列的长度小于低阈值时，不丢弃报文；当队列的长度在低阈值和高阈值之间时，RED开始随机丢弃报文，队列的长度越长，丢弃的概率越高；当队列的长度大于高阈值时，丢弃所有的报文

➤ WRED 加权随机早期检测

WRED与RED的区别在于：WRED引入了IP优先集和IP DSCP值来区分丢弃策略，可以为不同的IP优先级和IP DSCP值设定不同的队列长度、队列阈值、丢弃概率，从而对不同优先级的报文提供不同的丢弃特性。这是WRED的重要特点

4.1.6. 实验安全配置

➤ 优先级队列(PQ)的实验配置

```
Router(config)# priority-list 1 protocol ip high tcp 5500
Router(config)# priority-list 1 protocol ip low tcp www
Router(config)# priority-list 1 protocol ip medium
Router(config)# priority-list 1 default normal
Router(config)# priority-list 1 queue-limit 20 40 60 80 //配置队列数据包的深度
Router(config-if)# priority-group 1
```

查看命令： Router# show queueing priority //查看优先级队列配置

➤ 自定义队列(CQ)的实验配置

```
Router(config)# queue-list 1 protocol ip 0 tcp 5500
Router(config)# queue-list 1 protocol ip 1 tcp www
Router(config)# queue-list 1 protocol ipv6 2
Router(config)# queue-list 1 protocol pppoe 3
Router(config)# queue-list 1 default 4
Router(config)# queue-list 1 queue 1 byte-count 15000 //配置 1 号队列的尺寸为 15K
Router(config-if)# custom-queue-list 1
Router# show queueing custom //查看自定义队列配置
```

➤ 基于类的加权公平队列(CBWFQ)的实验配置

实验目的：限制源自 192.168.10.0/24 的流量的带宽为 1000kbps

```
Router(config)# class-map match-all TRAIN //class-map 是用来定义流量
Router(config-cmap)# match access-group 19 //定义指定的 IP 流量
Router(config)# access-list 19 permit 192.168.10.0 0.0.0.255
```

```
Router(config)# policy-map ZL-TRAIN //定制策略
Router(config-pmap)# class TRAIN //调用 class-map 定义的流量
Router(config-pmap-c)# bandwidth 1000k //限制最高带宽为 1000k
Router(config-pmap-c)# queue-limit 30 //队列数据上限为 30
Router(config-pmap)# class class-default //其它为默认的(一定要配置)
```

```
Router(config)# interface s0/0
Router(config-if)# ip add 172.16.1.19 255.255.255.0
Router(config-if)# service-policy output ZL-TRAIN //在接口下应用
```

实验的调用过程：1、接口下使用 service-policy 调用 policy-map

2、policy-map 调用 class-map

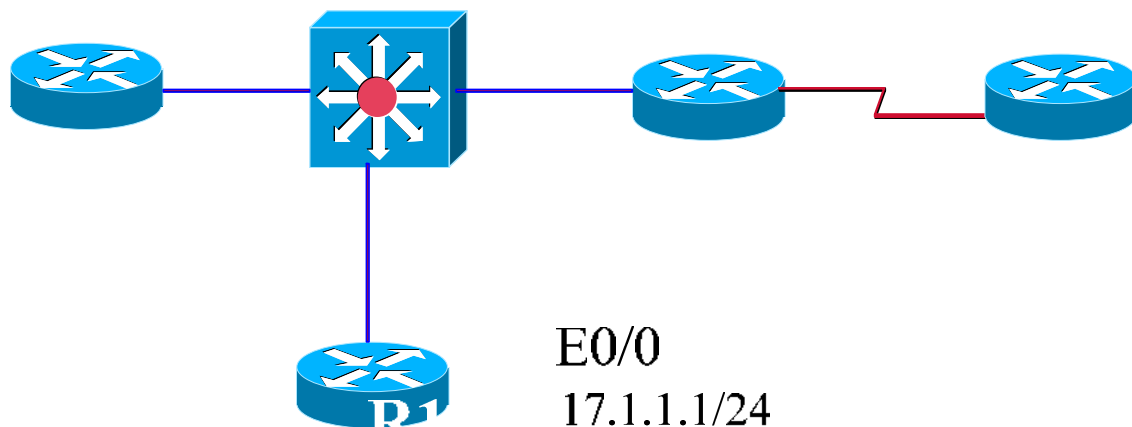
3、class-map 调用 access-list

配置 CBWFQ (实验图为下图所示)

实验要求：a. 由 R1 发送到 R4 的流量进行限速 10K 每秒

b. 由 R2 发送到 R4 的流量进行 drop (丢弃)处理

c. 由其它流量可以正常转发



配置为:

```
R1(config)# no ip routing
R1(config)# ip default-gateway 17.1.1.3
R1(config)# interface e0/0
R1(config-if)# ip address 17.1.1.1 255.255.255.0
R1(config-if)# no shutdown
```

R2 配置为:

```
R2(config)# no ip routing
R2(config)# ip default-gateway 17.1.1.3
R2(config)# interface e0/0
R2(config-if)# ip address 17.1.1.2 255.255.255.0
R2(config-if)# no shutdown
```

17.1.1.2/24
E0/0

R3 配置为:

```
//配置相关接口地址信息
R3(config)# interface e0/0
R3(config-if)# ip address 17.1.1.3 255.255.255.0
R3(config-if)# no shutdown
R3(config)# interface s0/0
R3(config-if)# ip address 34.0.0.1 255.255.255.252
R3(config-if)# no shutdown
```

//定义 ACL 和两个 class-map

```
R3(config)# class-map match-all TRAIN
R3(config-cmap)# match access-group 19
R3(config)# access-list 19 permit 17.1.1.1
R3(config)# class-map match-all TRAIN01
R3(config-cmap)# match access-group 20
R3(config)# access-list 20 permit 17.1.1.2
```

//定义 policy-map 策略

```
R3(config)# policy-map ZL-TRAIN
R3(config-pmap)# class TRAIN
R3(config-pmap-c)# bandwidth 10 //限制为 10K
```

```
R3(config-pmap-c)# exit
R3(config-pmap)# class TRAIN01
R3(config-pmap-C)# drop    //丢弃
R3(config-pmap)# class class-default    //默认流量以默认转发规则
R3(config-pmap)# end
```

//应用策略到指定的接口方向

```
R3(config-if)# service-policy output ZL-TRAIN
```

//测试方法:

```
R1#ping ip
```

```
Target IP address: 34.0.0.2
```

```
Repeat count [5]: 10000    //发送数据包的个数为 10000
```

```
Datagram size [100]: 18024    //设定字节数为 18K
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]:
```

```
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
```

```
Sending 10000, 18024-byte ICMP Echos to 34.0.0.2,
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
R2#ping ip
```

```
Target IP address: 34.0.0.2
```

```
Repeat count [5]:
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]:
```

```
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 34.0.0.2, timeout is 2 seconds:
```

```
.....    //结果被丢弃了
```

```
Success rate is 0 percent (0/5)
```

//在 R3 上查看应用结果:

```
R3#show policy-map interface s0/0
```

```
Serial0/0
```

```
Service-policy output: ZL-TRAIN
```

```
Class-map: TRAIN (match-all)
```

```
85882 packets, 120991748 bytes
```

```
5 minute offered rate 351000 bps, drop rate 0 bps
```

```
Match: access-group 19
```

```
Queueing
```

```
Output Queue: Conversation 265
```

```
Bandwidth 10 (kbps) Max Threshold 30 (packets)
```

```
(pkts matched/bytes matched) 72660/101116860
```

```
(depth/total drops/no-buffer drops) 3/0/0
```

```

Class-map: TRAIN01 (match-all)
  16 packets, 1664 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group 20
  drop

```

```

Class-map: class-default (match-any)
  272 packets, 19008 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any

```

4.2.CAR(承诺访问速率)

4.2.1. CAR(承诺访问速率)

对于 ISP 来说对用户送入网络中的流量进行控制是十分必要的。对于企业网，对某些应用的流量进行控制也是一个有力的控制网络状况的工具，网络管理者可以使用约定访问速率 CAR 来对流量进行控制。

CAR通常使用在网络边界路由器的接口上，用来限制进入或离开该网络的流量速率。每个接口可以配置多个CAR策略，当数据包进入使用了多个策略的接口时，路由器将检查每个策略，直到数据包和某个策略相匹配；如果没有找到匹配的策略，默认操作是转发该数据包。.

CAR 的使用限制：第一、CAR 只能对 IP 流量限速。第二、CAR 不支持快速以太网信道 (Fast EtherChannel) 第三、CAR 不支持隧道接口。第四、CAR 不支持 ISDN PRI 接口。

在边缘路由器上设定限速

//针对整个接口进行限速

```
R3(config-if)#rate-limit input 1000000 187500 375000 conform-action transmit exceed-action drop
```

```
R3(config-if)#rate-limit output 1000000 187500 375000 conform-action transmit exceed-action drop
```

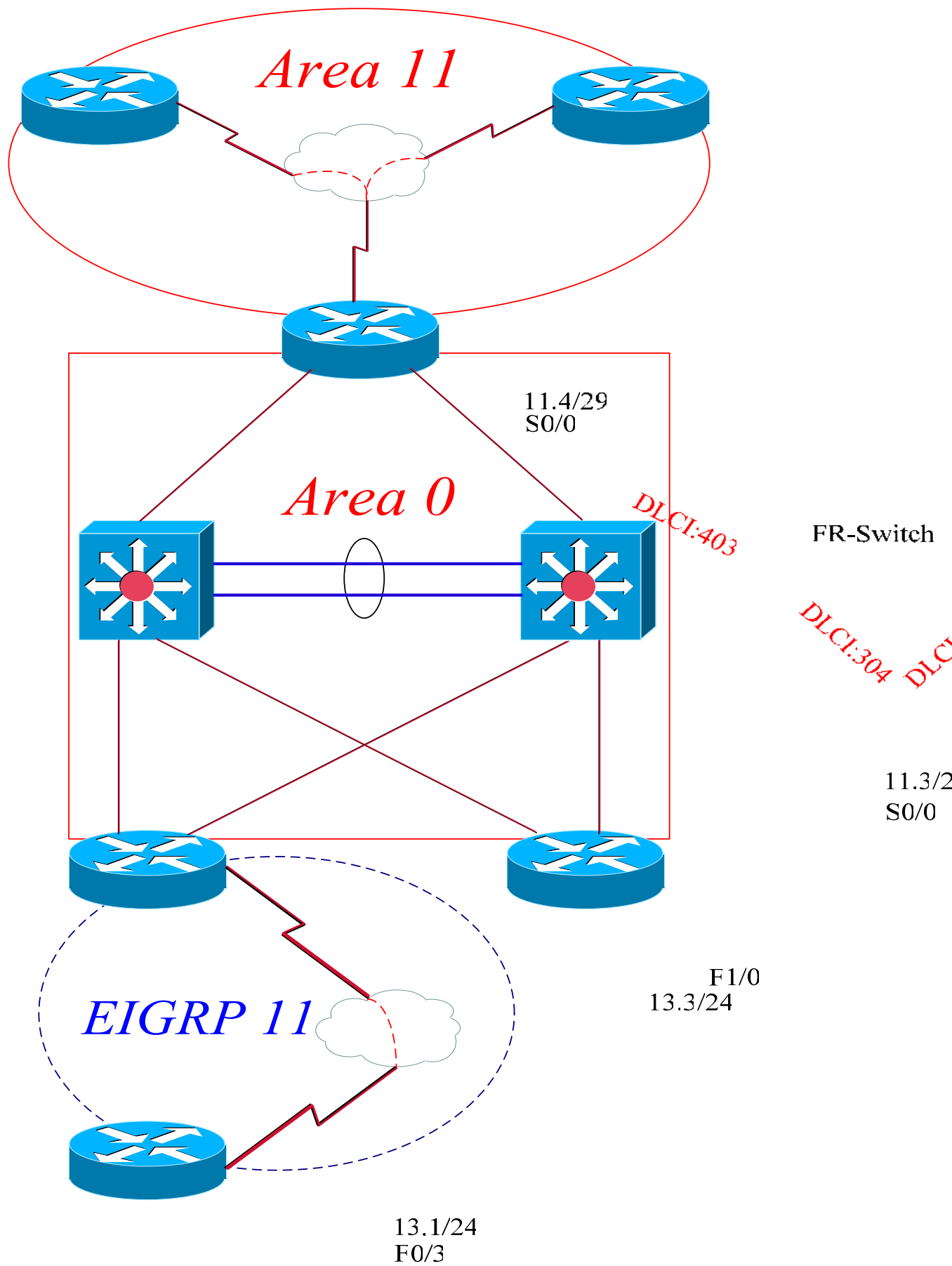
//针对某个 IP 地址或地址段进行限速，需要 ACL 支持

```
R3(config-if)#rate-limit input access-group 19 1000000 187500 375000 conform-action transmit
exceed-action drop
```

```
R3(config-if)#rate-limit output access-group 19 1000000 187500 375000 conform-action transmit
exceed-action drop
```

```
R3(config)# access-list 19 permit 17.1.1.1
```

4.3. 拓扑图制作及综合实验



F0/1 1

4.3.1. 配置步骤:

- 1、关闭所有路由器的 Console 接口超时

```
Router(config)# line con 0
```

```
Router(config-line)# exec-timeout 0 0
```

```
Router(config-line)# logging synchronous
```

- 2、配置各帧中继链路(例)

```
R1(config)# interface s0/0
```

```
R1(config-if)# ip address 1.1.16.1 255.255.255.0
```

```
R1(config-if)# encapsulation frame-relay
```

```
R1(config-if)# no arp frame-relay
```

```
R1(config-if)# no frame-relay inverse-arp
```

```
R1(config-if)# no shutdown
```

```
R1(config-if)# frame-relay map ip 1.1.16.6 106 broadcast
```

注意: 要保证各帧中继之间的直连链路必须连通, 切记!!

- 3、从上往下, 开始配置以太网接口, 保证各以太网接口之间的链路没有任何问题

- 4、在 Switch 上划分 VLAN, 保证各 VLAN 间的通信

- 5、在所有链路都已经全部连通的情况下, 开始配置路由协议

- 6、从 R1 到 SW2 的每一台设备上各配置一个 Loopback 接口的地址, 例如: 1.1.XX-1.1.8.8

- 7、配置 OSPF, 从主干区域开始, 保证主干区域之间的所有邻居能够正常建立

8、配置 OSPF 的常规区域, 保证能够正常建立邻居关系(特别提示: NBMA 的网络需要使用 Neighbor 命令来指定邻居, 因为 NBMA 的网络是不能够自动发现的邻居, 另外, 要保证 R3 的 S0/0 接口成为 DR, R4 与 R5 的接口不能成为 DR)

- 9、配置 EIGRP 路由协议(在 R1 上, 发布 EIGRP 时, 需要带掩码发布)

- 10、实现双向路由重发分, 且要保证每一台路由或交换机都能够 ping 通其它设备。

- 11、将 OSPF 的常规区域 Area11 配置为: 完全末节区域(Totally Stubby Area)。

4.3.2. 整个实验的完整配置

R1 的完整配置

```
R1(config)# interface Loopback0
```

```
R1(config-if)# ip address 1.1.1.1 255.255.255.255
```

```
R1(config)# interface Serial0/0
```

```
R1(config-if)# ip address 1.1.16.1 255.255.255.0
```

```
R1(config-if)# encapsulation frame-relay
```

```
R1(config-if)#no arp frame-relay
```

```
R1(config-if)# frame-relay map ip 1.1.16.6 106 broadcast
```

```
R1(config-if)# no frame-relay inverse-arp
```

```
R1(config)# interface FastEthernet1/0
```

```
R1(config-if)# ip address 1.1.12.1 255.255.255.0
```

```
R1(config)# interface FastEthernet2/0
```

```
R1(config-if)# ip address 1.1.21.1 255.255.255.0
```

```
R1(config)# router eigrp 11
```

```
R1(config-router)# redistribute ospf 1 metric 100000 1000 255 1 1500
R1(config-router)# network 1.1.16.0 0.0.0.255
R1(config-router)# no auto-summary
```

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# redistribute eigrp 11 metric 10 subnets
R1(config-router)# network 1.1.1.1 0.0.0.0 area 0
R1(config-router)# network 1.1.12.1 0.0.0.0 area 0
R1(config-router)# network 1.1.21.1 0.0.0.0 area 0
```

R2 的完整配置

```
R2(config)# interface Loopback0
R2(config-if)# ip address 1.1.2.2 255.255.255.255
R2(config)# interface FastEthernet0/0
R2(config-if)# ip address 1.1.12.2 255.255.255.0
R2(config)# interface FastEthernet1/0
R2(config-if)# ip address 1.1.21.2 255.255.255.0
```

```
R2(config)# router ospf 1
R2(config-router)# router-id 1.1.2.2
R2(config-router)# network 1.1.2.2 0.0.0.0 area 0
R2(config-router)# network 1.1.12.2 0.0.0.0 area 0
R2(config-router)# network 1.1.21.2 0.0.0.0 area 0
```

R3 的完整配置

```
R3(config)# interface Loopback0
R3(config-if)# ip address 1.1.3.3 255.255.255.255
R3(config)# interface Serial0/0
R3(config-if)# ip address 1.1.11.3 255.255.255.248
R3(config-if)# encapsulation frame-relay
R3(config-if)# ip ospf priority 255
R3(config-if)# no arp frame-relay
R3(config-if)# frame-relay map ip 1.1.11.4 304 broadcast
R3(config-if)# frame-relay map ip 1.1.11.5 305 broadcast
R3(config-if)# no frame-relay inverse-arp
```

```
R3(config)# interface FastEthernet1/0
R3(config-if)# ip address 1.1.13.3 255.255.255.0
R3(config)# interface FastEthernet2/0
R3(config-if)# ip address 1.1.31.3 255.255.255.0
```

```
R3(config)# router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)# area 11 stub no-summary
R3(config-router)# network 1.1.3.3 0.0.0.0 area 0
```



```
R3(config-router)# network 1.1.11.3 0.0.0.0 area 11
R3(config-router)# network 1.1.13.3 0.0.0.0 area 0
R3(config-router)# network 1.1.31.3 0.0.0.0 area 0
R3(config-router)# neighbor 1.1.11.4
R3(config-router)# neighbor 1.1.11.5
```

R4 的完整配置

```
R4(config)# interface Loopback0
R4(config-if)# ip address 1.1.4.4 255.255.255.255
R4(config)# interface Serial0/0
R4(config-if)# ip address 1.1.11.4 255.255.255.248
R4(config-if)# encapsulation frame-relay
R4(config-if)# ip ospf priority 0
R4(config-if)# no arp frame-relay
R4(config-if)# frame-relay map ip 1.1.11.3 403 broadcast
R4(config-if)# frame-relay map ip 1.1.11.5 403
R4(config-if)# no frame-relay inverse-arp
```

```
R4(config)# router ospf 1
R4(config-router)# router-id 1.1.4.4
R4(config-router)# area 11 stub
R4(config-router)# network 1.1.4.4 0.0.0.0 area 11
R4(config-router)# network 1.1.11.4 0.0.0.0 area 11
```

R5 的完整配置

```
R5(config)# interface Loopback0
R5(config-if)# ip address 1.1.5.5 255.255.255.255
R5(config)# interface Serial0/0
R5(config-if)# ip address 1.1.11.5 255.255.255.248
R5(config-if)# encapsulation frame-relay
R5(config-if)# ip ospf priority 0
R5(config-if)# no arp frame-relay
R5(config-if)# frame-relay map ip 1.1.11.3 503 broadcast
R5(config-if)# frame-relay map ip 1.1.11.4 503 broadcast
R5(config-if)# no frame-relay inverse-arp
```

```
R5(config)# router ospf 1
R5(config-router)# router-id 1.1.5.5
R5(config-router)# area 11 stub no-summary
R5(config-router)# network 1.1.5.5 0.0.0.0 area 11
R5(config-router)# network 1.1.11.5 0.0.0.0 area 11
```

R6 的完整配置

```
R6(config)# interface Loopback0
R6(config-if)# ip address 1.1.6.6 255.255.255.255
R6(config)# interface Serial0/0
R6(config-if)# ip address 1.1.16.6 255.255.255.0
R6(config-if)# encapsulation frame-relay
R6(config-if)# no arp frame-relay
R6(config-if)# frame-relay map ip 1.1.16.1 601 broadcast
R6(config-if)# no frame-relay inverse-arp

R6(config)# router eigrp 11
R6(config-router)# network 1.0.0.0
R6(config-router)# network 6.0.0.0
R6(config-router)# no auto-summary
```

SW1 的完整配置

```
SW1(config)# ip routing
SW1(config)# interface Loopback0
SW1(config-if)# ip address 1.1.7.7 255.255.255.255
SW1(config)# interface FastEthernet0/1
SW1(config-if)# switchport access vlan 10
SW1(config-if)# spanning-tree portfast
SW1(config)# interface FastEthernet0/2
SW1(config-if)# switchport access vlan 10
SW1(config-if)# spanning-tree portfast
SW1(config)# interface FastEthernet0/3
SW1(config-if)# no switchport
SW1(config-if)# ip address 1.1.13.1 255.255.255.0
SW1(config)# interface FastEthernet0/11
SW1(config-if)# switchport access vlan 100
SW1(config)# interface FastEthernet0/12
SW1(config-if)# switchport access vlan 100
SW1(config)# interface Vlan10
SW1(config-if)# ip address 1.1.12.254 255.255.255.0
SW1(config)# interface Vlan100
SW1(config-if)# ip address 100.0.0.1 255.255.255.252

SW1(config)# router ospf 1
SW1(config-router)# router-id 1.1.7.7
SW1(config-router)# network 1.1.7.7 0.0.0.0 area 0
SW1(config-router)# network 1.1.12.254 0.0.0.0 area 0
SW1(config-router)# network 1.1.13.1 0.0.0.0 area 0
SW1(config-router)# network 100.0.0.1 0.0.0.0 area 0
```

SW2 的完整配置

```
SW2(config)# interface Loopback0
SW2(config-if)# ip address 1.1.8.8 255.255.255.255
SW2(config)# interface FastEthernet0/1
SW2(config-if)# switchport access vlan 20
SW2(config-if)# spanning-tree portfast
SW2(config)# interface FastEthernet0/2
SW2(config-if)# switchport access vlan 20
SW2(config-if)# spanning-tree portfast
SW2(config)# interface FastEthernet0/3
SW2(config-if)# no switchport
SW2(config-if)# ip address 1.1.31.1 255.255.255.0
SW2(config)# interface FastEthernet0/11
SW2(config-if)# switchport access vlan 100
SW2(config)# interface FastEthernet0/12
SW2(config-if)# switchport access vlan 100
SW2(config)# interface Vlan20
SW2(config-if)# ip address 1.1.21.254 255.255.255.0
SW2(config)# interface Vlan100
SW2(config-if)# ip address 100.0.0.2 255.255.255.252

SW2(config)# router ospf 1
SW2(config-router)# router-id 1.1.8.8
SW2(config-router)# network 1.1.8.8 0.0.0.0 area 0
SW2(config-router)# network 1.1.21.254 0.0.0.0 area 0
SW2(config-router)# network 1.1.31.1 0.0.0.0 area 0
SW2(config-router)# network 100.0.0.2 0.0.0.0 area 0
```