标度教育 思科网络工程师培训

CCNA 实验手册

编写：标度教育•课程研发组

www.chinaiplab.com

1. 前言

我们应该怎样学习Cisco认证课程

当你来到标度IP实验室学习Cisco认证课程时，可能会感到以前学习的内容基本派不上用场,这是十分正常的。因为大学注重理论知识的传授，实习操作难免会大打折扣。标度IP实验室将秉承理论与实际相结合的教学理念，为学员提供优质的课程。当然，要真正掌握Cisco认证课程的内容，学员需要认真努力做到以下几点:

1、上课时认真听讲，做好课堂笔记。遇到听不懂的问题，可以马上向老师或周围的同学请教，当天的问题，当天解决。

2、晚上应该抽出十几分钟，把今天的课堂笔记翻一下，回忆老师讲过的内容。如果发现有不太明白的地方，马上记录下来，第二天问老师或同学。

3、每周应该对本周的课堂笔记进行小结，比如学到了哪些重要的命令，每个命令的应用场合、参数、作用等。构建属于你的知识网，形成你自己的知识体系。

4、经常与老师、同学交流。不论是技术方面，还是生活中的困难我们都要及时沟通，这样可以避免自己钻牛角尖，白白浪费时间和精力。很快你就会发现，标度IP实验室的老师待人是那么的真诚、同学们之间是那么的热心互助，这里的一切都会让你感觉到家的温馨!

5、学会在网上淘金，登陆标度IP实验室论坛，从其他学员的课堂笔记、实验报告上提取精华，取长补短，拾遗补缺，可以少走弯路，抓住重点。

当你做到了以上几点，就会感到学习思科的技术并不是像自己一开始想象的那么难，而是很容易。总之，所有问题，通过自己的努力和老师的帮助，我们都可以找到答案。只要充满信心，勤奋努力，克服困难，就可以掌握思科技术，实现自己的目标。

2. 实验环境介绍

2.1. 实验手册使用说明

该实验手册是面向标度IP实验室CCNA学员的内部学习材料，所有的路由实验均有由三台路由器组成，交换实验则由四台交换机构成全互联结构，基本上涵盖了CCNA学习所必需的的实验内容。

该实验手册约有80个实验，共由五部分组成。第一部分为实验环境介绍，重点介绍实验室拓扑结构，终端服务器的使用方法，以及WireShark的使用方法；第二部分是路由基础篇，重点在于介绍路由器的访问方法和基本配置；第三部分是路由协议和概念篇，重点介绍了静态路由、RIP、EIGRP、OSPF的基本内容和系列实验；第四部分是LAN交换和无线篇，重点介绍了交换机的工作原理、生产树协议、VLAN等，以及无线局域网的相关内容，提供了丰富的实验；第五部分是接入WAN篇，重点介绍了当前流行的广域网接入技术、网络安全和ACL、ADSL技术，以及IP编址技术，提供了大量的实验。

实验手册的使用建议:

本实验手册没有完全给出完整的配置命令，目的在于让学员能够加强对配置的熟练程度，以及增强脱离书本后的动手能力;

本实验手册中存在人为和非人为的错误，目的在于让学员能够发现问题，加深对实验的理解;

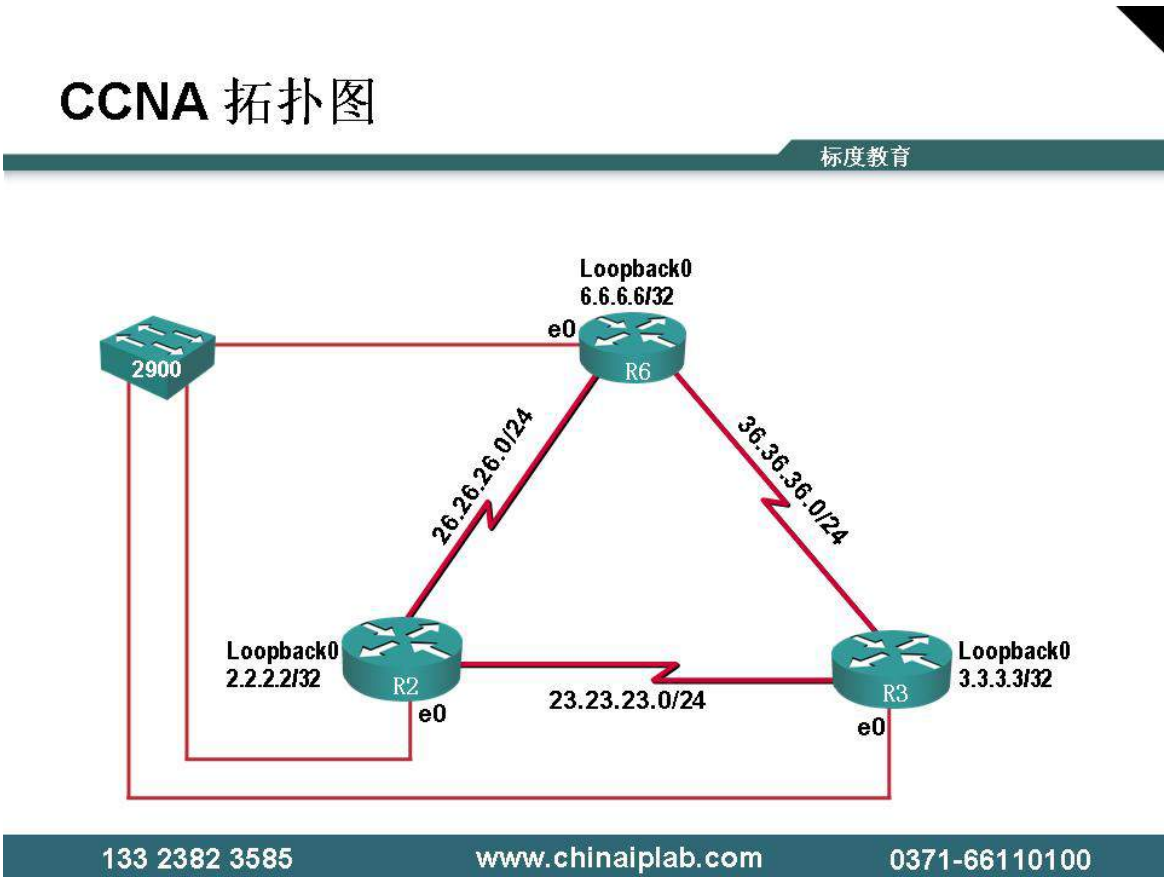
对于在试验中发现的问题，希望学员指正。

标度教育•课程研发组

2010-01-01

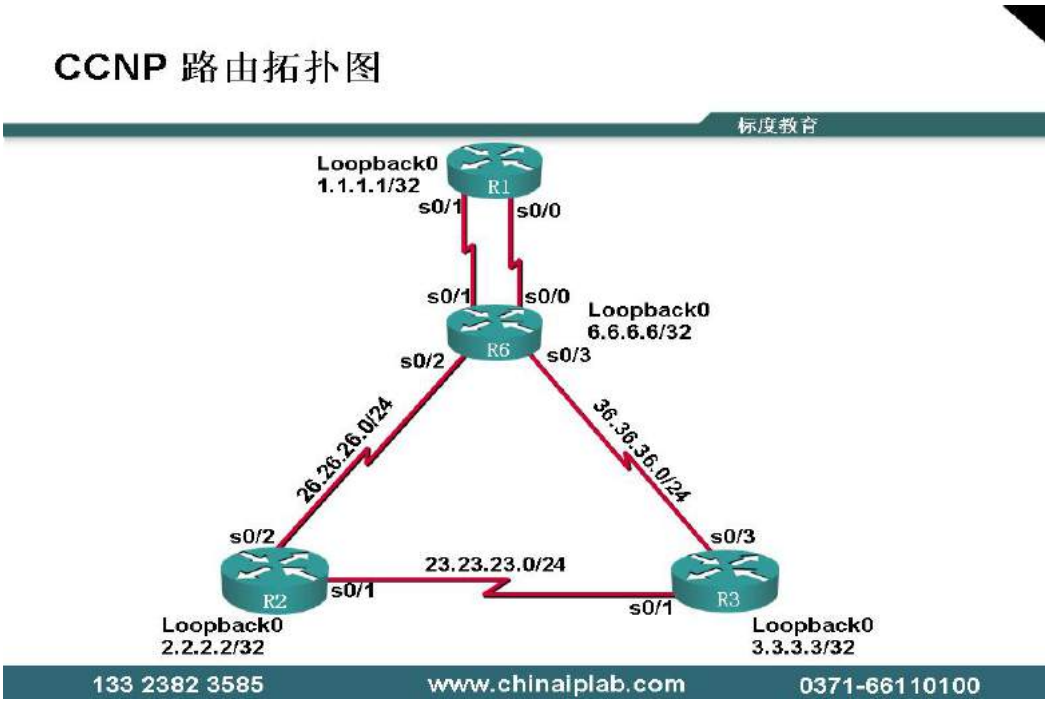
2.2. 实验室环境说明

2.2.1. CCNA实验拓扑



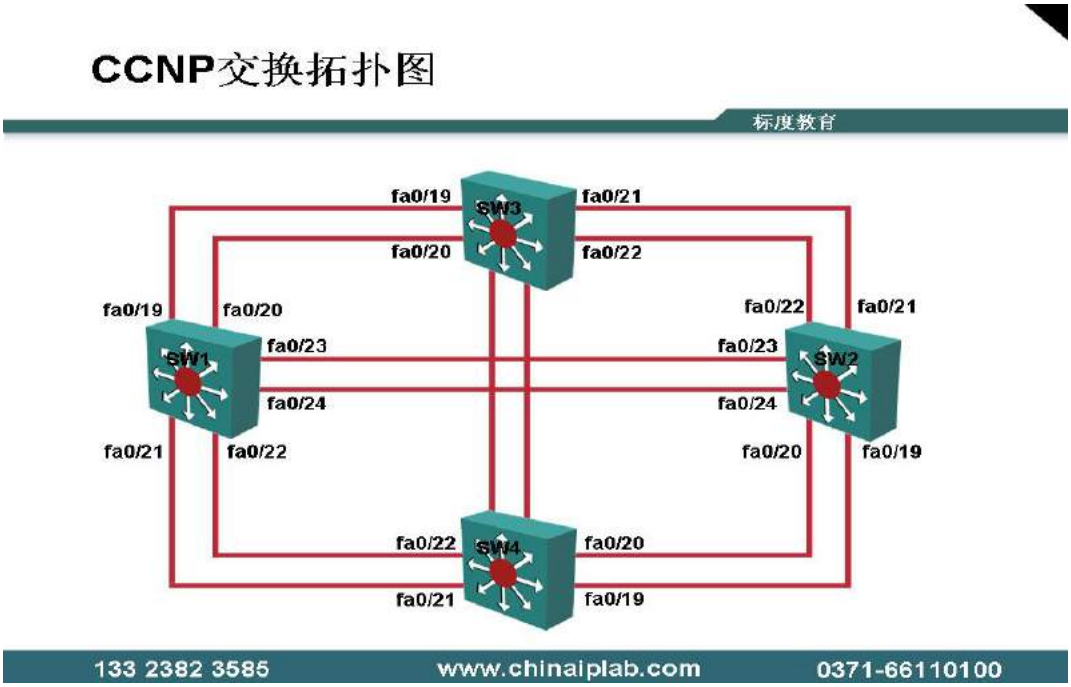
本实验拓扑由三台cisco 2501路由器和一台cisco catalyst 2900交换机组成，可以完成CCNA所有的路由交换实验。

2.3. CCNP路由实验拓扑



本实验拓扑由四台cisco 3640路由器组成，可以完成CCNP所有路由实验。

2.3.1. CCNP交换实验拓扑

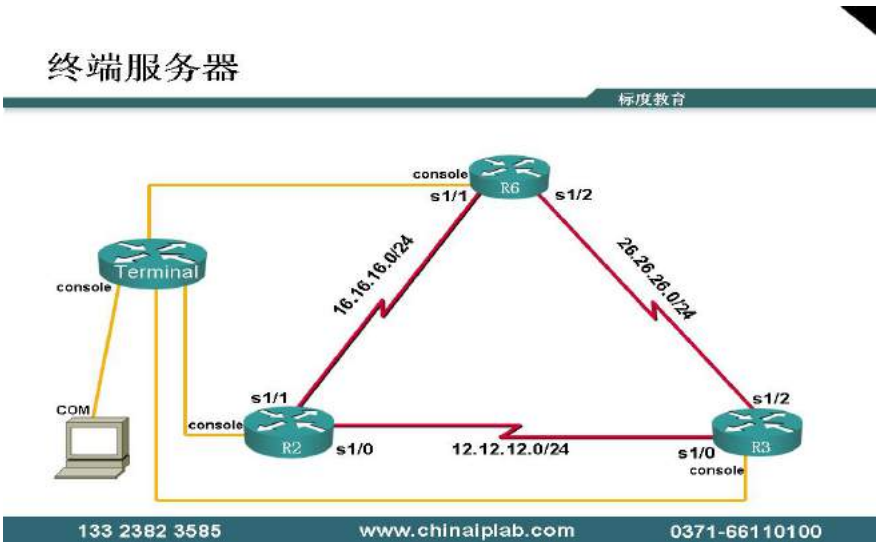


本实验拓扑由四台Cisco Catalyst 3550交换机组成，采取全互连的方式连接，可以完成CCNP所有交换实验。

2.4. 终端服务器的使用方法

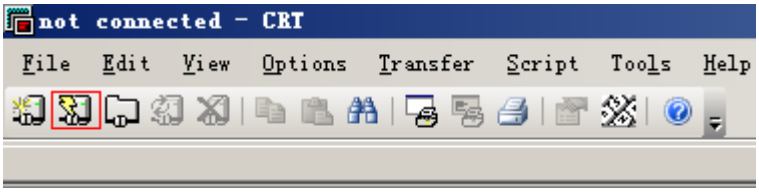
2.4.1. 实验室拓扑图

本实验室的所有实验设备都是通过终端服务器进行控制的。实验时可以采取telnet的方式登录到终端服务器上，通过终端服务器操控其它设备。其连接方式如下图所示：

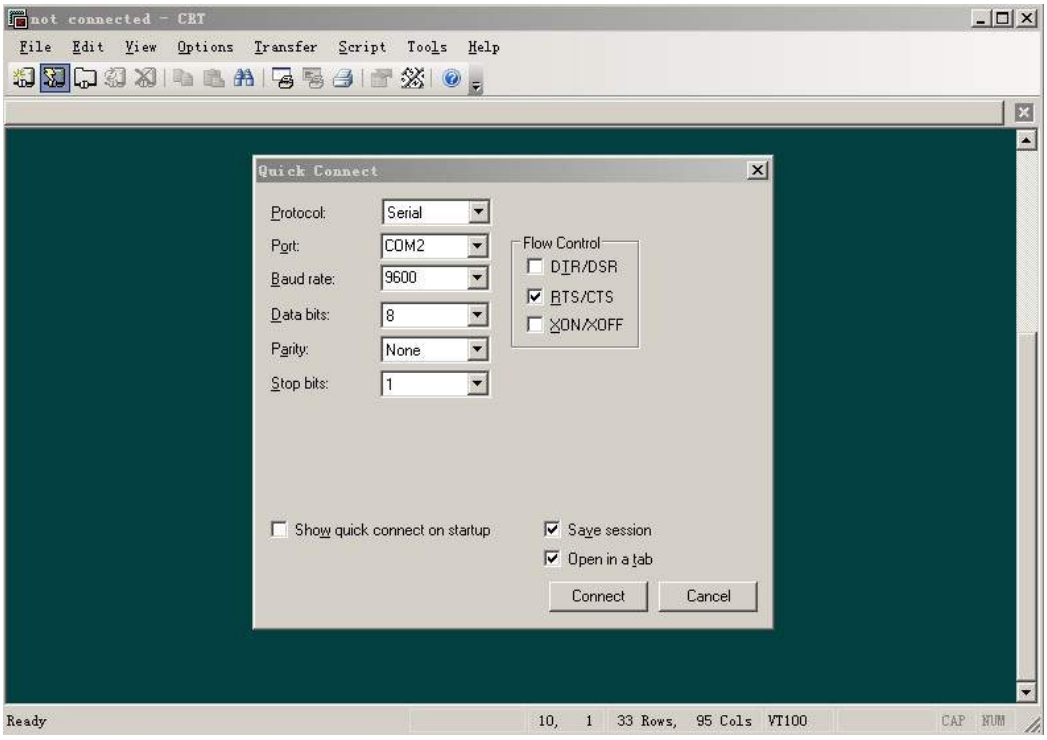


2.4.2. SecureCRT使用方法

上图中，PC通过com口使用控制线（console线）与终端服务器的console口相连。我们可以通过超级终端（SecureCRT ）与终端服务器建立连接，如下图所示：



点击红色方块中的按钮，出现如下对话框:



然后点击**connect**即可与终端服务器建立连接，成功建立连接后如下图所示:

在这里我们输入**cisco**即可登陆到终端服务器上，如下图所示:

我们从以上的输出中能看到链接到这台终端服务器上的设备，在这里我们可以输入相应设备的名字，进入到该设备，如要登陆到**R6**上进行配置，只需要输入**R6**，回车即可登陆到**R6**上，成功登陆**R6**后的的画面如下:

如果还要登陆其它设备，此时我们可以同时按住**ctrl+shift+6**，释放后按**x**，将先前建立的会话挂起，此时我们会重新回到终端服务器的状态，如下图所示:

此时我们只要输入相应设备的名称即可登陆。依次方法，可以登陆到多台设备。在这里提供

几个在终端服务器上使用的命令:

Show line用于查看目前使用的线路

Show session用于查看当前已经建立的会话，以及正在进行的会话

Clear line用于清除相应的线路

2.5. WireShark的使用方法

2.5.1. 实验目的

掌握基本的网络协议分析方法。通过抓包工具，观察Mac帧、IP包格式。

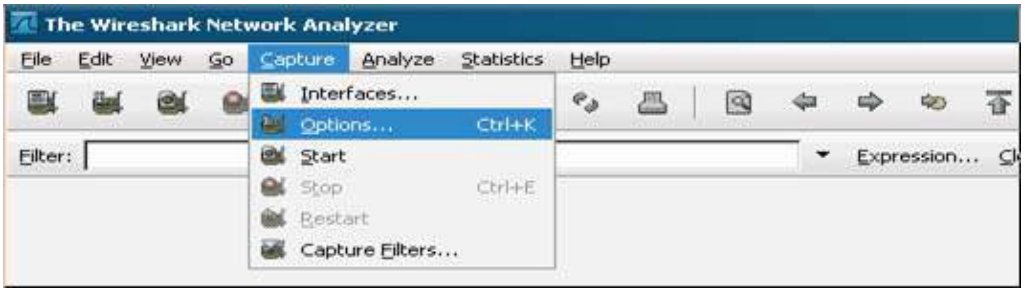
2.5.2. 实验环境

网络实验室局域网，安装Windows2000/XP操作系统之PC机。

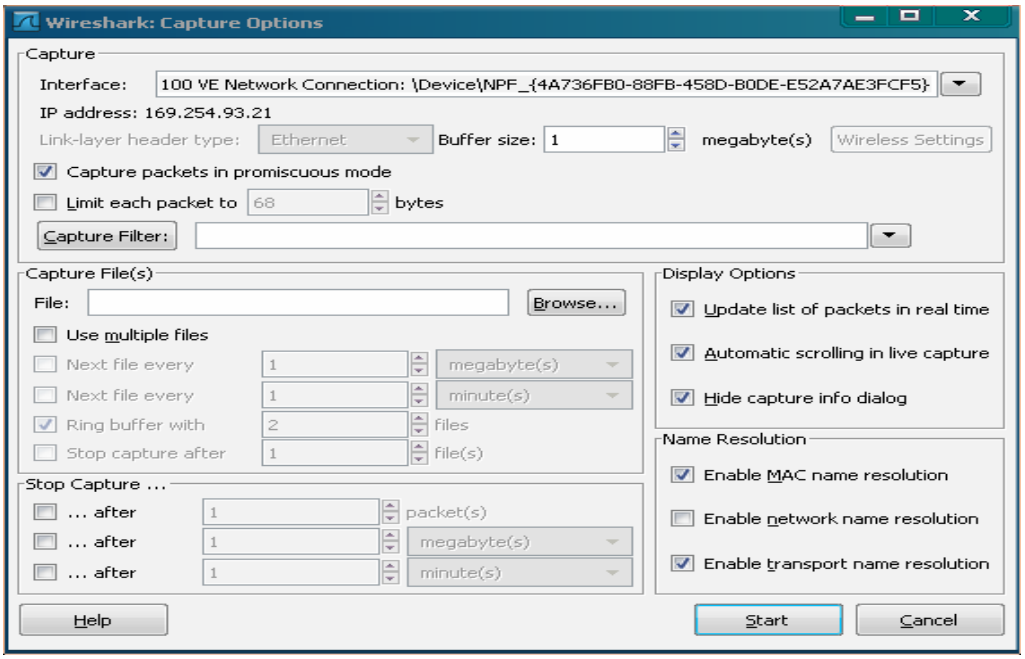
2.5.3. 实验步骤

2.5.4. 启动Wireshark

如图所示：启动Wireshark后，需要选择当前需要监视的网卡

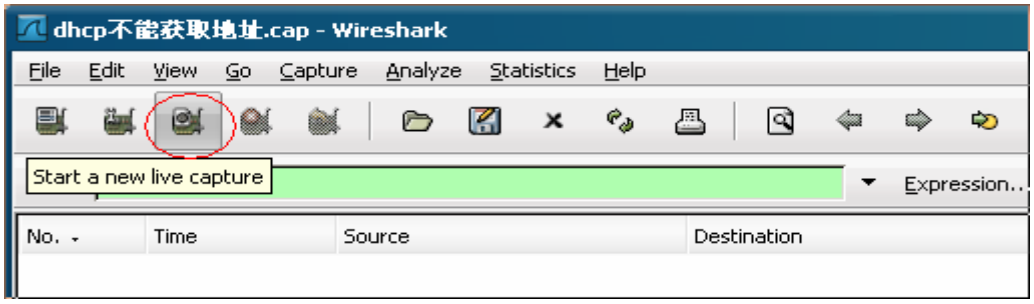


启动后，如图所示:



2.5.5. 开始抓包

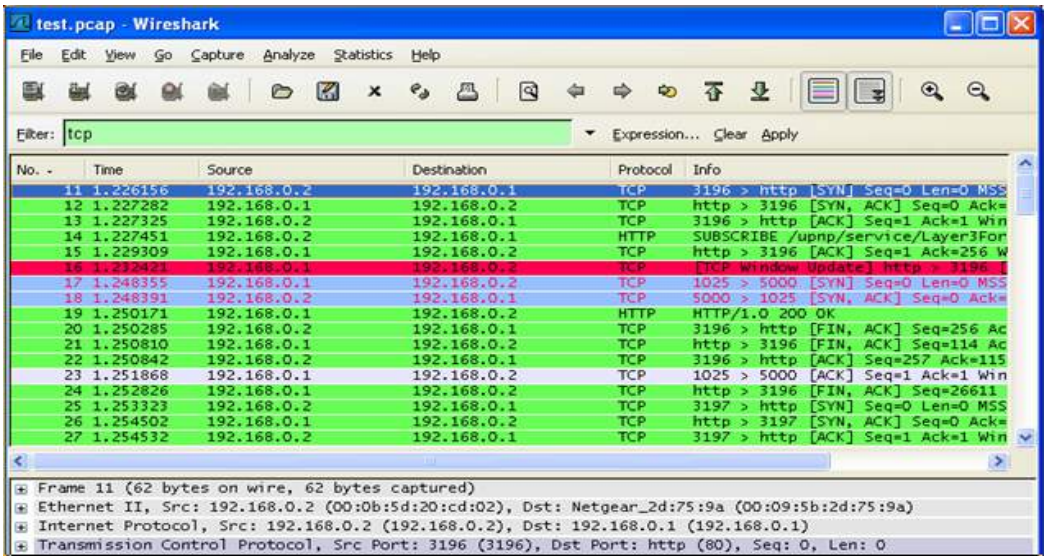
点击上图中菜单行第三行中的▲按钮，启动抓包过程；如下图所示;



为配合抓包，此时，需要打开IE浏览器，访问一个WWW网站.

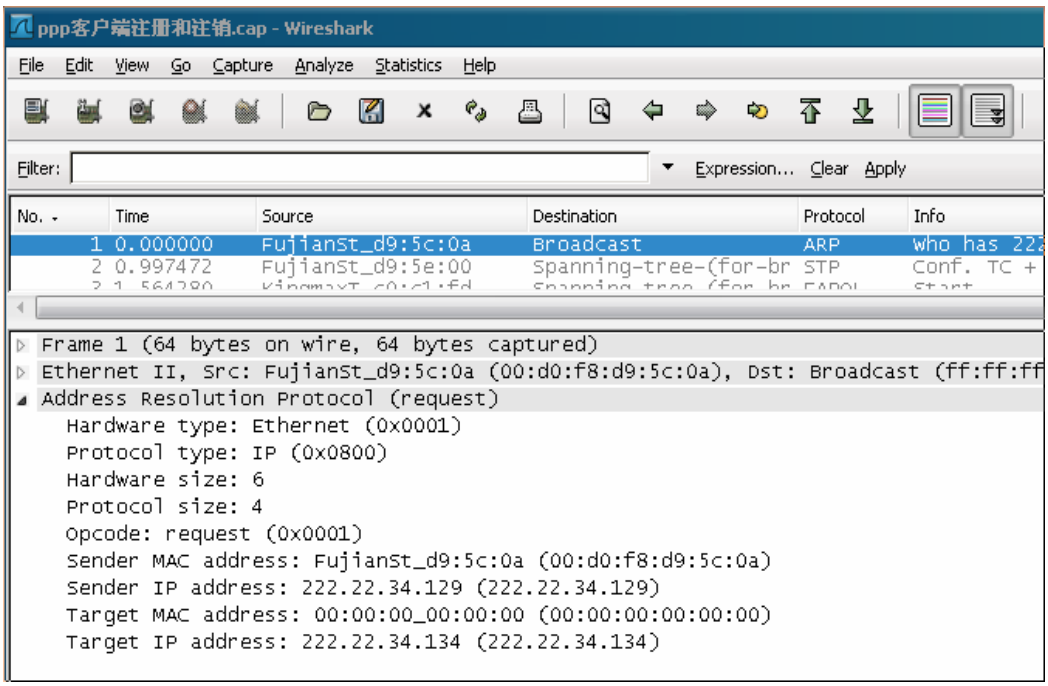
2.5.6. Filtering packets while viewing

Wireshark有两种过滤语言:一种是抓包的时候用,一种是抓包之后用来显示包的时候用.
我们现在讨论一下第二种用法:显示过滤.
这种用法允许你以下内容进行包的显示过滤:
Protocol,协议
The presence of a field,存在的字段
The values of fields,字段的值
A comparison between fields,字段的对照比较
... and a lot more!,以及其他更多的内容
... and a lot more!
下面是一个基于Protocol字段来过滤TCP数据的例子
你可以看到,只有TCP包被显示出来

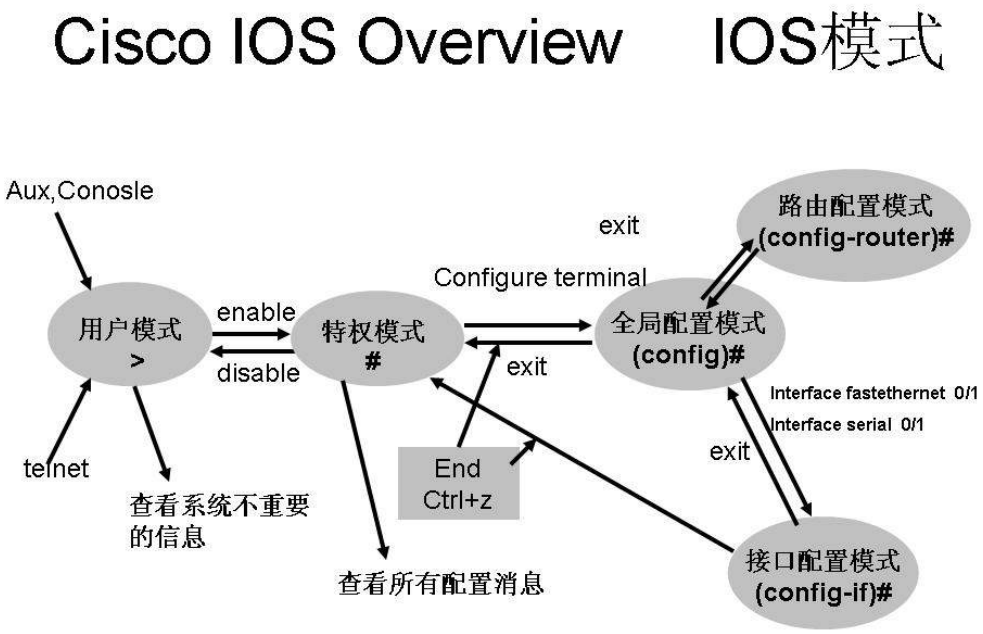


2.5.7. 观察、分析Mac帧、IP包格式

点击你所感兴趣的数据包，即可观察到**Wireshark**所捕获的**Mac**帧、**IP**包，对照课程中所介绍的相应帧、包格式作进一步分析。



2.6. Cisco IOS Overview



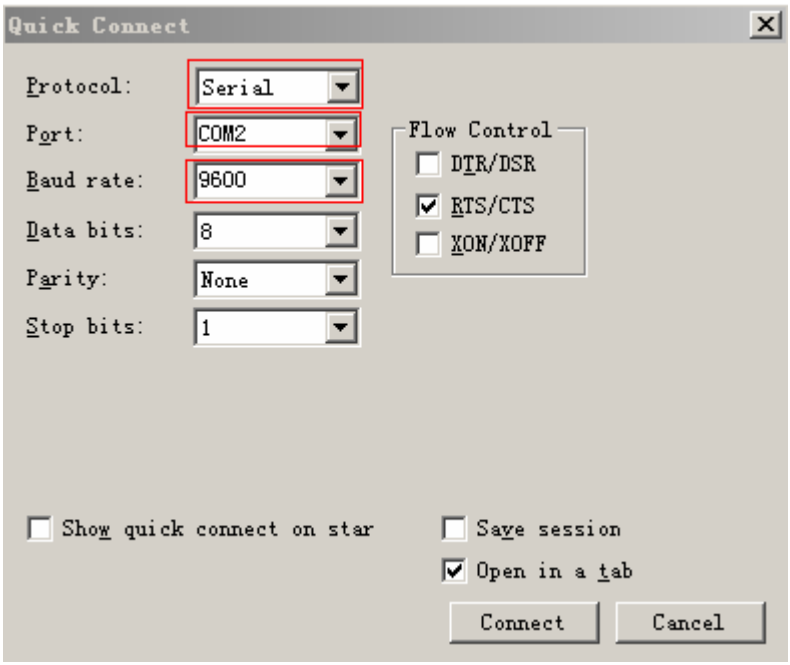
3. 路由基础篇

3.1. 访问Cisco路由器

3.1.1. 通过Console口访问路由器

使用**console**线将路由器的**console**口和**PC**机的**DB-9**串行接口相连;

打开**SecureCRT**，点击**File—Quick Connect**，出现如下图所示对话框，选择**Port**的编号与你本机的编号（通过查看本机设备管理器可知）要一致，**Baud bits**要选择**9600**，其它无需修改，然后点击右下角**Connect**即可:



3.2. 通过Telnet访问路由器

- 检查你的**PC**机到所要连接的路由器连通性，通过**ping**该设备的**ip**地址即可，如**ping 1.1.1.11**。
- 要想通过**Telnet**访问路由器，首先必须通过**Console**进入路由器，并为**VTY**线路配置访问口令，此外还需要为路由器配置特权模式访问用户名和口令。

基本配置如下:

R6(config)#line vty 0 4……线路数目与 IOS 版本有关，根据需要自行选择
R6(config-line)#login……指定登陆时需要验证口令
% Login disabled on line 130, until 'password' is set
% Login disabled on line 131, until 'password' is set
% Login disabled on line 132, until 'password' is set
% Login disabled on line 133, until 'password' is set
% Login disabled on line 134, until 'password' is set
R6(config-line)#password cisco……配置 Telnet 登陆口令
R6(config-line)#exit
R6(config)#enable pass chinaiplab……配置特权模式访问口令
R6(config)#int fa0/1
R6(config-if)#ip address 1.1.1.11 255.255.255.0

R6(config-if)#no shutdown

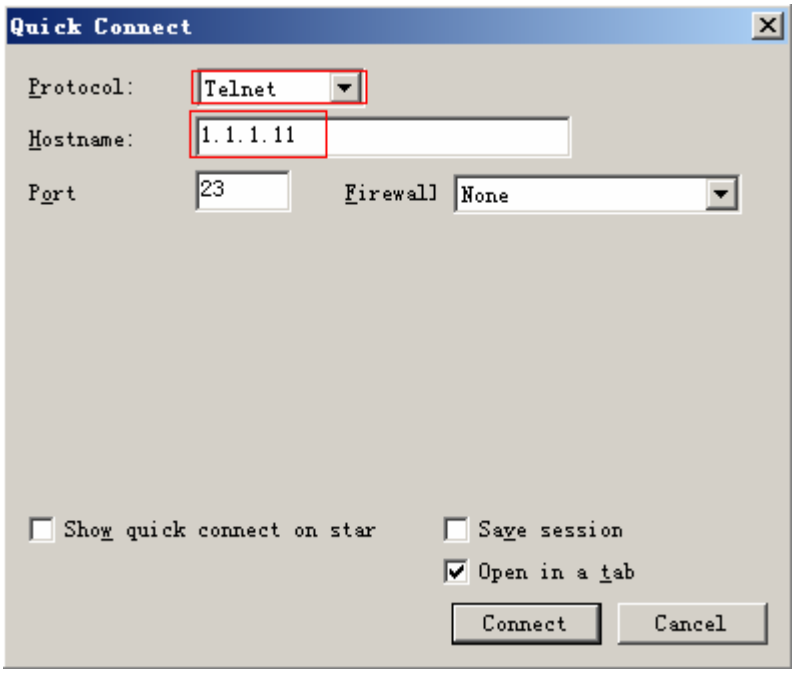
如果没有配置 Telnet 登陆口令，将会出现下面的现象：

Trying 1.1.1.11 ... Open

Password required, but none set

如果没有配置特权模式访问口令，将只能登陆到设备上，而无法对其进行操作，因此必须配置 password 或 secret 密码。

1、 打开 SecureCRT，点击 File—Quick Connect，出现如下图所示对话框，Protocol 选择 Telnet，Hostname 要选择你所要连接 1.1.1.11，其它无需修改，然后点击右下角 Connect 即可：



正确配置后，登陆时将会出现以下输出：

Trying 26.26.26.6 ... Open

User Access Verification

Password: ……此处输入 cisco，但是不会显示

R6>en

Password: ……此处输入 chinaiplab，同样不会显示

R6#……成功 Telnet 到 R6，并进入特权模式

1.1 通过 AUX 口访问路由器

- **通过AUX口访问路由器与通过Console口访问基本一致，唯一的区别是：通过AUX口访问需要用户名和口令。**
- **默认时，通过Console口访问路由器是不需要任何用户名和口令的。我们可以先通过Console口进入路由器，并为AUX口设定访问口令，这样我们才能正常通过AUX口访问路由器。**

基本配置：

- R6(config)#line aux 0
- R6(config-line)#password chinaiplab
- 通过 Console 连接 PC 机与路由器 R6 的 AUX，将会提示输入登陆口令，输入 chinaiplab 即可访问。

3.3. 路由器基本配置

3.3.1. CLI的使用与IOS基本命令

登陆路由器后，常用的基本命令如下：

Router>enable……从用户模式进入特权模式
Router#configure terminal……从特权模式进入配置模式
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R6……给路由器命名为 R6
R6(config)#no ip domain-lookup ……关闭域名查找功能
R6(config)#interface serial 0/1……进入接口模式
R6(config-if)#ip add 172.16.1.1 255.255.255.0……给接口配置 IP 地址
R6(config-if)#no shutdown ……激活接口
R6(config-if)#clock rate 64000……给接口配置始终频率
R6(config-if)#end……退到特权模式
R6#

3.3.2. 配置文件的管理和IOS的管理

路由器的配置文件存放在NVRAM中，当路由器启动时要去查找存放在NVRAM中的配置文件，就相当于启动windows时要查找硬盘中的操作系统一样。启动后路由器会将NVRAM中的配置文件copy一份放到RAM中。我们对路由器的操作只会临时保存在RAM中，要使得我们的配置在路由器重启后依然生效，就必须使用命令copy running-config startup-config将配置保存到NVRAM。

以下是配置文件管理的相关命令:

R6#copy running-config startup-config……将配置保存到NVRAM
Destination filename [startup-config]? ……回车
Building configuration...
[OK]
R6#copy tftp startup-config……将TFTP服务器中的配置文件恢复到NVRAM

IOS是路由器的镜像文件，就相当于PC机windows操作系统，因此也有IOS的更新，恢复，重新加载等。以下是相关命令:

R6#copy tftp flash……将TFTP服务器上的IOS恢复到路由器的flash中
R6#copy flash tftp……将flash中的IOS备份到TFTP服务器中

3.4. 密码恢复和IOS的恢复

3.4.1. 路由器的两种密码

路由器的密码有两种，secret和password。默认情况下password密码以明文显式，通过show running-config可以查看，而secret密码默认启用MD5加密，show running-config只能看到加密后的密文。以下是密码配置及查看:

R6(config)#enable pass cisco
R6(config)#enable secret ccna
R6#sh run
Building configuration...
【output omitted】
enable secret 5 $1$4zY6$shfn9oQGulKUP9EajPkVW.……密文显式

enable password cisco……明文显式

3.4.2. 密码的遗忘恢复

一旦我们将密码遗忘或丢失，只能通过密码恢复的方式删除，之后才能正常登陆到设备。Cisco不同的设备破解密码的方式稍有不同，大致步骤是重新启动路由器，60秒内按ctrl+break进入监控模式，将寄存器的值改成0x2142，保存并重启，最后就可以正常登陆设备，使用如下命令可以清楚原有的口令;

R6(config)#no enable pass

R6(config)#no enable secret

此后可以重新配置设备的登陆口令。

3.4.3. 路由器的IOS恢复

路由器的IOS相当于PC机的操作系统，一旦损坏或丢失，路由器将无法正常工作，因此需要重新加载。Cisco不同设备IOS加载方式不大一样，以下是cisco 3600系列恢复IOS的方法:

首先启动路由器，60秒内按ctrl+break进入监控模式，然后执行以下命令。

rommon 1 > confreg 回车

Configuration Summary
enabled are:
load rom after netboot fails
console baud: 9600
boot: image specified by the boot system commands
or default to: cisco2-C2600
do you wish to change the configuration? y/n [n]: y (选择 yes)
enable "diagnostic mode"? y/n [n]: n (选择 no)
enable "use net in IP bcast address"? y/n [n]: n (选择 no)
disable "load rom after netboot fails"? y/n [n]: n (选择 no)
enable "use all zero broadcast"? y/n [n]: n (选择 no)
enable "break/abort has effect"? y/n [n]: n (选择 no)
enable "ignore system config info"? y/n [n]: n (选择 no)
change console baud rate? y/n [n]: y (选择 yes)
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: 7 (选择 7,用最大的 115200 速率的 xmodem 传输)
change the boot characteristics? y/n [n]: n (选择 no)
Configuration Summary
enabled are:
load rom after netboot fails
console baud: 115200
boot: image specified by the boot system commands
or default to: cisco2-C2600
do you wish to change the configuration? y/n [n]: n (选择 no)
You must reset or power cycle for new config to take effect
rommon 2 > reset 回车

3.5. CDP配置

1、CDP（cisco discovery protocol，思科发现协议），是基于数据链路层的协议，用于发现拓扑结构，该协议是cisco私有，因此无法在其他厂家设备上使用。

2、配置CDP非常简单，默认情况下cisco设备开启CDP，因此我们无需做任何配置，只需要将设备的所有接口都激活，然后通过命令show cdp neighbors查看CDP邻居表，并根据此表获悉网络拓扑结构。

```
R6#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2               Ser 0/2           173          R S I      3640      Ser 0/2
```

从以上邻居表可以获悉一下信息，路由器R6同过接口serial0/2连接到R2的serial0/2接口。其他的信息如设备的型号，保持时间等在此不做介绍。

3.6. 实验环境参考配置

实验环境拓扑结构参见3.1。

以下实验如未做特殊说明，基本配置均采用以下配置。

以下是参考配置:

```
R6#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R6(config)#int loopback 0
R6(config-if)#ip add 6.6.6.6 255.255.255.0
R6(config)#int s0/3
R6(config-if)#ip add 36.36.36.6 255.255.255.0
R6(config-if)#no sh
R6(config-if)#clock rate 64000……时钟频率只需要在 DCE 接口上配置
R6(config)#int s0/2
R6(config-if)#ip add 26.26.26.6 255.255.255.0
R6(config-if)#no sh

R2#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R2(config)#int loopback 0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config)#int s0/2
R2(config-if)#ip add 26.26.26.2 255.255.255.0
R2(config-if)#no sh
R2(config)#int s0/1
R2(config-if)#ip add 23.23.23.2 255.255.255.0
R2(config-if)#no sh

R3#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R3(config)#int loopback 0
```

```
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config)#int s0/3
R3(config-if)#ip add 36.36.36.3 255.255.255.0
R3(config-if)#no sh
R3(config)#int s0/1
R3(config-if)#ip add 23.23.23.3 255.255.255.0
R3(config-if)#no sh
```

接口是否为DCE，可以通过命令show controllers [interface type|number]查看。

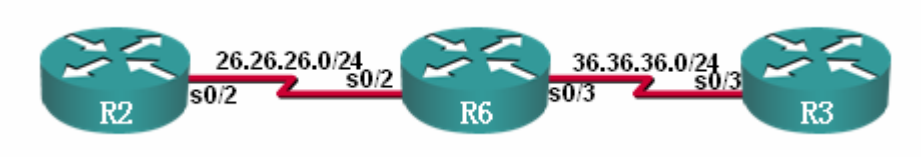
4. 路由协议和概念篇

4.1. 静态路由与动态路由协议概述

4.1.1. 带下一跳地址的静态路由

1、 静态路由的特点是需要管理员手工配置，占用设备 CPU、内存的资源少，适用于小型网络。

2、 实验拓扑



3、 以下是静态路由的配置方法：

R2(config)#ip route 36.36.36.0 255.255.255.0 26.26.26.6

R3(config)#ip route 26.26.26.0 255.255.255.0 36.36.36.6

4、 验证：

R2#ping 36.36.36.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 36.36.36.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 44/68/96 ms

R2#sh ip route

【output omitted】

36.0.0.0/24 is subnetted, 1 subnets

S 36.36.36.0 [1/0] via 26.26.26.6

26.0.0.0/24 is subnetted, 1 subnets

C 26.26.26.0 is directly connected, Serial0/2

R3#ping 26.26.26.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 26.26.26.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/66/92 ms

在这个实验重要注意的是，静态路由的配置一般是双向的，如果只配置其中一个方向，如在R3上删除静态路由R3(config)#no ip route 26.26.26.0 255.255.255.0 36.36.36.6，然后在R2上将无法ping 36.36.36.3成功，然而此时R2的路由表并未发生变化。

4.1.2. 带出接口的静态路由

1、 R2、R6 基本配置和实验拓扑与 9.1 一致。

2、 R3 上配置的静态路由如下：

R3(config)# ip route 26.26.26.0 255.255.255.0 s0/1

此时，在 R6 上 ping 23.23.23.3 和在 R3 上 ping 26.26.26.6 都能成功，对比 R3 和 R6 的路由表：

R6#sh ip route

【output omitted】

23.0.0.0/24 is subnetted, 1 subnets

S 23.23.23.0 [1/0] via 26.26.26.2

R3#sh ip route

【output omitted】

26.0.0.0/24 is subnetted, 1 subnets

S 26.26.26.0 is directly connected, Serial0/1

带下一跳 IP 地址的静态路由的管理距离是 1，而带送出接口的静态路由管理距离为 0，即如上所显示的 directly。

4.1.3. 浮动静态路由

1、 浮动静态路由本身是静态路由，浮动的含义是当原来的路由失效，该静态路由才开始启用，因此在配置浮动静态路由时，需要将其管理距离做相应的调整，使得其大于正常使用的其他路由协议获悉的路由。

2、 实验拓扑：

3、 本实验中采用 RIP 协议，RIP 的配置参考 RIP 章节。

4、 当完成配置后，查看路由表发现，R6 的路由表如下：

R6#sh ip route

【output omitted】

23.0.0.0/24 is subnetted, 1 subnets

S 23.23.23.0 [1/0] via 26.26.26.2……由于在 R6 上配置了 ip route 23.23.23.0 255.255.255.0 26.26.26.2，因此出现该路由

26.0.0.0/24 is subnetted, 1 subnets

C 26.26.26.0 is directly connected, Serial0/2

发现去往 23.23.23.0 网络，仍然是通过静态路由的，并没有出现 RIP 路由。原因是静态路由的管理距离小于 RIP（120），因此，我们需要将该静态路由的管理距离调整到大于 120，该实验中调整为 130。

R6(config)#ip route 23.23.23.0 255.255.255.0 26.26.26.2 130

此时 R6 的路由表如下：

R6#sh ip route

【output omitted】

23.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

S 23.23.23.0/24 [130/0] via 26.26.26.2

R 23.0.0.0/8 [120/1] via 26.26.26.2, 00:00:21, Serial0/2

26.0.0.0/24 is subnetted, 1 subnets

C 26.26.26.0 is directly connected, Serial0/2

虽然静态路由和 RIP 同时存在，但是由于此时静态路由的管理距离为 130，大于 RIP，所以该静态路由将不会启用。

我们通过增加 ACL 的方式模拟 RIP 路由 down 的情况，配置如下：

R6(config)#access-list 101 deny udp 26.26.26.2 255.255.255.0 26.26.26.6 255.255.255.0 eq 520

R6(config)#access-list 101 permit ip any any

R6(config)#int s0/2

R6(config-if)#ip access-group 101 in

此时我们查看 R6 的路由表发现，通过 RIP 学习到的路由从路由表中删除了，

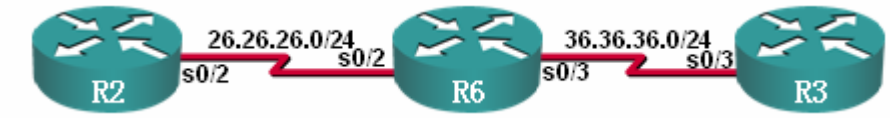
R6#sh ip route
【output omitted】
23.0.0.0/24 is subnetted, 1 subnets
S 23.23.23.0 [130/0] via 26.26.26.2
26.0.0.0/24 is subnetted, 1 subnets
C 26.26.26.0 is directly connected, Serial0/2
R6 与 R3 的连通性也没有受到影响
R6#ping 23.23.23.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 23.23.23.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/87/136 ms

4.2. RIP

4.2.1. RIPv1基本配置

1、 实验中用到的 show 命令有 show ip protocols，show ip route，show ip rip database。
2、 实验拓扑：



3、 基本配置：
R6# router rip
R6(config-router)# network 6.6.6.0
R6(config-router)# network 26.26.26.0
R6(config-router)# network 36.36.36.0

R2(config)# router rip
R2(config-router)# network 2.2.2.0
R2(config-router)# network 26.26.26.0

R3(config)# router rip
R3(config-router)# network 3.3.3.0
R3(config-router)# network 36.36.36.0
4、 通过相关 show 命令进行检验：
R2#sh ip route
【output omitted】
2.0.0.0/24 is subnetted, 1 subnets
C 2.2.2.0 is directly connected, Loopback0
R 3.0.0.0/8 [120/2] via 26.26.26.6, 00:00:21, Serial0/2
R 36.0.0.0/8 [120/1] via 26.26.26.6, 00:00:21, Serial0/2
R 6.0.0.0/8 [120/1] via 26.26.26.6, 00:00:21, Serial0/2
26.0.0.0/24 is subnetted, 1 subnets
C 26.26.26.0 is directly connected, Serial0/2

在 R2 上 pingR3 的 loopback 0 的 ip 地址 3.3.3.3，

R2#ping 3.3.3.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/76/128 ms

4.2.2. 被动接口与单播更新

1、 完成基本的 RIP 配置，参考上个实验。

2、 配置被动接口：

R2(config-router)#passive-interface s0/2

R6(config-router)#passive-interface s0/2

R6(config-router)#passive-interface s0/3

R3(config-router)#passive-interface s0/3

此时查看执行 clear ip route *命令，发现 R2，R3 和 R6 的路由表中已经没有 RIP 路由，R2 也不能再 ping 3.3.3.3 成功。

3、 如果要解决上面的问题，需要再配置单播更新：

R2(config-router)#neighbor 26.26.26.6

R6(config-router)#neighbor 26.26.26.2

在这里并未配置R6和R3之间的单播更新，此时R2上ping 6.6.6.6成功，但是ping 3.3.3.3不成功，R2的路由表中只有从R6获悉的关于6.6.6.0和36.36.36.0网络（注意：此时并不能ping 36.36.36.3成功）。如果要使得所有路由器之间都能通信，必须配置所有的单播更新。

4.2.3. RIPv2基本配置

1、 RIPv2 和 RIPv1 的配置基本一致，只需要额外声明版本号。

2、 基本配置：

R6(config)# router rip

R6(config-router)#version 2……配置 RIP 为第 2 版本

R6(config-router)# network 6.6.6.0

R6(config-router)# network 26.26.26.0

R6(config-router)# network 36.36.36.0

R2(config)# router rip

R2(config-router)#version 2

R2(config-router)# network 2.2.2.0

R2(config-router)# network 26.26.26.0

R3(config)# router rip

R3(config-router)#version 2

R3(config-router)# network 3.3.3.0

R3(config-router)# network 36.36.36.0

3、 验证：

通过 show ip route 查看路由表，

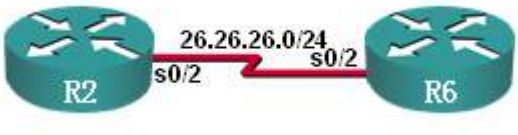
R2#sh ip route

2.0.0.0/24 is subnetted, 1 subnets
C 2.2.2.0 is directly connected, Loopback0
R 3.0.0.0/8 [120/2] via 26.26.26.6, 00:00:26, Serial0/2
R 36.0.0.0/8 [120/1] via 26.26.26.6, 00:00:26, Serial0/2
R 6.0.0.0/8 [120/1] via 26.26.26.6, 00:00:26, Serial0/2
26.0.0.0/24 is subnetted, 1 subnets
C 26.26.26.0 is directly connected, Serial0/2

4.2.4. RIPv2手工总结、验证和触发更新

1、 RIPv2 是无类协议，支持可变字长掩码（VLSM），而 RIPv1 是有类协议，只支持固定长度的子网掩码。因此在 RIPv2 中可以执行手工汇总，而 RIPv1 不能。此外 RIPv2 默认开启自动汇总。

2、 实验拓扑：



3、 手动汇总的基本配置：

首先在 R2 上增加多个 loopback 接口，IP 地址分别配置 192.168.1.33/27，192.168.1.66/27，192.168.1.99/27，最后将他们汇总为 192.168.1.0/24。

```
R2(config)#int looopback 1
R2(config-if)#ip add 192.168.1.33 255.255.255.224
R2(config)#int looopback 2
R2(config-if)#ip add 192.168.1.66 255.255.255.224
R2(config)#int looopback 3
R2(config-if)#ip add 192.168.1.99 255.255.255.224
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.1.32
R2(config-router)#network 192.168.1.64
R2(config-router)#network 192.168.1.96
R2(config-router)#network 26.26.26.0
R2(config-router)#network 2.2.2.0
R2(config-router)#no auto-summary……关闭默认汇总
```

```
R6(config)#router rip
R6(config-router)#version 2
R6(config-router)#network 26.26.26.0
R6(config-router)#network 6.6.6.0
R6(config-router)#no auto
```

此时，我们查看 R6 上的路由表，

```
R6#sh ip route
【output omitted】
R 192.168.1.96 [120/1] via 26.26.26.2, 00:00:00, Serial0/2
R 192.168.1.64 [120/1] via 26.26.26.2, 00:00:00, Serial0/2
R 192.168.1.32 [120/1] via 26.26.26.2, 00:00:00, Serial0/2
```

发现，R6 通过 S0/2 从 R2 学习到了关于 192.168.1.32，192.168.1.64 和 192.168.1.96 这 3 个网络，我们可以在 R2 上执行手工汇总，使得 R2 只通告这条汇总路由 192.168.1.0 给 R6，配置如下，

R2(config)#int s0/2……向 R6 通告更新的接口

R2(config-if)#ip summary-address rip 192.168.1.0 255.255.255.0

此时 R6 的路由表如下：

R6#sh ip route

【output omitted】

R 192.168.1.0/24 [120/1] via 26.26.26.2, 00:00:03, Serial0/2

4、 RIPv2 沿用了 RIPv1 的更新机制，采用周期更新，每 30 秒发送一次包含整个路由表条目的更新。尽管如此，RIPv2 增加了新的机制，可以配置触发更新，只需要在通告更新的接口上配置命令：

R2(config)#int s0/2

R2(config-if)#ip rip triggered 即可实现触发更新，此时可以通过 show ip protocols 查看到 hold down 时间为 0。

R2# sh ip pro

Routing Protocol is "rip"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Sending updates every 30 seconds, next due in 22 seconds

Invalid after 180 seconds, hold down 0, flushed after 240

4.2.5. 向RIP网络中注入默认路由

1、 使用 ip default-network 向 RIP 网络中注入默认路由。

2、 实验拓扑：

3、 基本配置：

在 R3 上面配置一条静态路由 ip route 2.2.2.0 255.255.255.0 loopback0

在 R6 上面通过“ip default-network”向 R2 注入默认路由

4、 验证：

要求在 R6 上面看到一条“C*”的路由

在 R2 上看到一条“R*”的路由

注意：

“ip default-network”命令后面的网络一定要是主类网络；

“ip default-network”后面的网络可以是直连的或者通过其他协议学到的网络。

4.2.6. RIPv2认证

1、 RIPv2 支持 MD5 认证。

2、 实验拓扑：

3、 基本配置：

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 2.2.2.0
R2(config-router)#network 26.26.26.0
R2(config)#int s0/2
R2(config-if)#ip rip authentication mode md5……启用 MD5 认证
R2(config-if)#ip rip authentication key-chain ccna……配置钥匙链 ccna
R2(config-if)#exit
R2(config)#key chain ccna
R2(config-keychain)#key 1……配置钥匙链 ccna 的一把钥匙
R2(config-keychain-key)#key-string chinaiplab……配置 key ID=1 的密钥
```

当配置完 R2 后，使用 clear ip route *清空路由表，发现 R2 的路由表中不再包含 6.0.0.0 的网络。这是由于 R6 还未配置，因此两端的认证出现错误。

```
R6(config)#router rip
R6(config-router)#version 2
R6(config-router)#network 6.6.6.0
R6(config-router)#network 26.26.26.0
R6(config)#int s0/2
R6(config-if)#ip rip authentication mode md5
R6(config-if)#ip rip authentication key-chain ccna
R6(config-if)#exit
R6(config)#key chain ccna
R6(config-keychain)#key 1
R6(config-keychain-key)#key-string chinaiplab
```

4、 验证：

```
R2#sh ip route
【output omitted】
R       6.0.0.0/8 [120/1] via 26.26.26.6, 00:00:26, Serial0/2
        26.0.0.0/24 is subnetted, 1 subnets
C           26.26.26.0 is directly connected, Serial0/
R2#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/36/88 ms
```

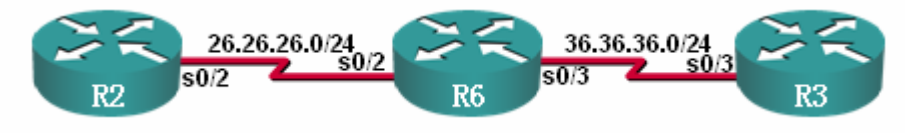
4.3. EIGRP

4.3.1. EIGRP基本配置

1、 EIGRP：增强型内部网关协议，是 cisco 私有的动态路由选择协议。它支持 VLSM，能够有效解决不连续子网，同时具有收敛速度快，触发更新等一系列有点，其配置步骤与 RIP 基本一致。此外 EIGRP 默认开启自动汇总。

2、 EIGRP 在配置时增加了一个新的概念——进程号，用于区别同一台路由器上不同的 EIGRP 进程。

3、 实验拓扑：



4、 基本配置：

R2(config)#router eigrp 100
R2(config-router)#network 2.2.2.0
R2(config-router)#network 26.26.26.0

R6(config)#router eigrp 100
R6(config-router)#network 6.6.6.0
R6(config-router)#network 26.26.26.0
R6(config-router)#network 36.36.36.0

R3(config)# router eigrp 100
R3(config-router)#network 3.3.3.0
R3(config-router)#network 36.36.36.0

5、 验证：以下是 R6 的路由表

R6#sh ip route
【output omitted】
2.0.0.0/24 is subnetted, 1 subnets
D 2.2.2.0 [90/2297856] via 26.26.26.2, 00:00:20, Serial0/2
D 3.0.0.0/8 [90/2297856] via 36.36.36.3, 00:03:15, Serial0/3
36.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 36.36.36.0/24 is directly connected, Serial0/3
D 36.0.0.0/8 is a summary, 00:03:30, Null0
6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 6.6.6.0/24 is directly connected, Loopback0
D 6.0.0.0/8 is a summary, 00:03:40, Null0
26.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 26.26.26.0/24 is directly connected, Serial0/2
D 26.0.0.0/8 is a summary, 00:03:40, Null0

由于 EIGRP 默认开启自动汇总，因此 3.3.3.0/24 被汇总为 3.0.0.0/8。

通过命令 show ip eigrp neighbours 查看邻居表。如下，R2 有 1 个邻居，是 R6，

R2#sh ip eigrp neighbors
IP-EIGRP neighbors for process 100

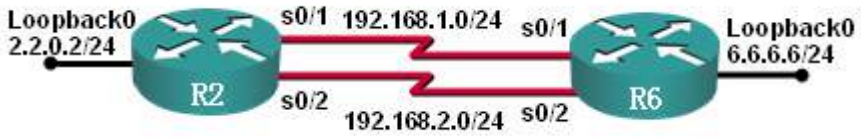
H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	26.26.26.6	Se0/2	14 00:35:12	76	684	0	26

此外可以通过 ping 来测试 3 台路由器之间的连通性。

4.3.2. EIGRP负载均衡

1、 当到达同一个目的地存在多条路径时，EIGRP 可以通过负载均衡来实现从多条路径同时转发数据，并能够在链路之间提供备份。负载均衡有等价和非等价之分。此实验只配置等价负载均衡。

2、 实验拓扑：



3、 基本配置：

R2(config)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#int s0/1
R2(config-if)#ip add 192.168.1.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#int s0/2
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#exit
R2(config)#router eigrp 1
R2(config-router)#net 2.2.2.0
R2(config-router)#net 192.168.1.0
R2(config-router)#net 192.168.2.0
R2(config-router)#no auto

R6(config)#int loo0
R6(config-if)#ip add 6.6.6.6 255.255.255.0
R6(config-if)#int s0/1
R6(config-if)#ip add 192.168.1.2 255.255.255.0
R6(config-if)#int s0/2
R6(config-if)#ip add 192.168.2.2 255.255.255.0
R6(config)#router eigrp 1
R6(config-router)#net 6.6.6.0
R6(config-router)#net 192.168.1.0
R6(config-router)#net 192.168.2.0
R6(config-router)#no auto

4、 验证

R2#sh ip route
【output omitted】
6.0.0.0/24 is subnetted, 1 subnets
D 6.6.6.0 [90/2297856] via 192.168.2.2, 00:00:04, Serial0/2
[90/2297856] via 192.168.1.2, 00:00:04, Serial0/1
R2 去往网络 6.6.6.0 有两条路径，其代价均为 2297856 等于 FD。
R2#sh ip eigrp topology
I【output omitted】
P 6.6.6.0/24, 2 successors, FD is 2297856
via 192.168.1.2 (2297856/128256), Serial0/1
via 192.168.2.2 (2297856/128256), Serial0/2
通过 R2#ping 6.6.6.6 source 2.2.2.2 repeat 20 查看，发现两条线路交替转发，每次一个
Dec 21 15:21:16.779: IP: s=2.2.2.2 (local), d=6.6.6.6 (Serial0/1), len 100, sending
Dec 21 15:21:16.803: IP: s=2.2.2.2 (local), d=6.6.6.6 (Serial0/2), len 100, sending
【output omitted】

4.3.3. EIGRP路由总结和EIGRP验证

1、 EIGRP 默认开启自动汇总，我们可以关闭自动汇总，采用手工汇总。EIGRP 支持 Null 认证，明文认证和 MD5 认证。

2、 实验拓扑：

3、 汇总的基本配置：此实验只用到 R2 和 R6，IP 编址参考 10.4

R2 和 R6 基本配置与 11.1 一致，额外在 R2 上增加了 3 个回环接口。如下，

```
R2(config)#int looopback 1
R2(config-if)#ip add 192.168.1.33 255.255.255.224
R2(config)#int looopback 2
R2(config-if)#ip add 192.168.1.66 255.255.255.224
R2(config)#int looopback 3
R2(config-if)#ip add 192.168.1.99 255.255.255.224
```

此时 R6 的路由表如下，

```
R6#sh ip route
【output omitted】
     192.168.1.0/27 is subnetted, 3 subnets
D       192.168.1.96 [90/2297856] via 26.26.26.2, 00:05:30, Serial0/2
D       192.168.1.64 [90/2297856] via 26.26.26.2, 00:05:30, Serial0/2
D       192.168.1.32 [90/2297856] via 26.26.26.2, 00:05:30, Serial0/2
```

4、 汇总验证：

在 R2 上执行手工汇总，将 192.168.1.32/27，192.168.1.64/27 和 192.168.1.96/27 汇总为 192.168.1.0/24。

```
R2(config)#int s0/2……向邻居通告更新的接口
R2(config-if)#ip summary-address eigrp 100 192.168.1.0 255.255.255.0
```

此时 R6 的路由表中就只存在上面这条汇总路由了，

```
R6#sh ip route
【output omitted】
D    192.168.1.0/24 [90/2297856] via 26.26.26.2, 00:00:06, Serial0/2
```

5、 MD5 认证配置：在 R2 和 R6 之间配置 MD5 认证。

```
R2(config)#int s0/2
R2(config-if)#ip authentication mode eigrp 100 md5……启用 MD5 认证
R2(config-if)#ip authentication key-chain eigrp 100 eigrp-md5……关联钥匙
```

此时 R2 和 R6 均会出现告警信息，两者的邻居关系也会 down，将无法通信。R2 上会出现 Neighbor 26.26.26.6 (Serial0/2) is down: authentication mode changed，这是由于 R6 还未配置 MD5 认证。

```
R2(config)#key chain eigrp-md5……定义钥匙链的名称 eigrp-md5
R2(config-keychain)#key 1……定义一把钥匙（可以定义多把）
R2(config-keychain-key)#key-string ccna……上面钥匙密钥为 ccna
```

R6 也要使用相同的配置，

```
R6(config)#int s0/2
R6(config-if)#ip authentication mode eigrp 100 md5
R6(config-if)#ip authentication key-chain eigrp 100 eigrp-md5
R6(config-if)#exit
R6(config)#key chain eigrp-md5
```

R6(config-keychain)#key 1
R6(config-keychain-key)#key-string ccna
6、 MD5 认证验证：
使用 show ip eigrp neighbours 查看邻居表，发现 R6 重新出现在邻居表中。
R2#sh ip eig nei
IP-EIGRP neighbors for process 100

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	26.26.26.6	Se0/2	13	00:00:05	101	606	0	43

R2 和 R6 之间的通信恢复正常，R6 的路由表中重新出现到达 R2 的相关条目。

4.3.4. 向EIGRP网络中注入默认路由

1、 该实验的配置方法与向 RIP 网络中注入默认路由基本一致。
2、 实验拓扑：

3、 该实验在上个实验的基础上进行。R2 和 R6 运行 EIGRP 100，R3 不运行任何动态路由选择协议，R3 和 R6 的默认路由如下，
R6(config)#ip route 0.0.0.0 0.0.0.0 36.36.36.3
R3(config)#ip route 0.0.0.0 0.0.0.0 36.36.36.6
在 R6 上将默认路由重分发进入 R2，
R6(config)#router eig 100
R6(config-router)#redistribute static metric 1544 20 255 1 1500，四个值分别是带宽，延迟，可靠性，负载和 MTU。配置完成后，在 R2 上测试，
R2#ping 3.3.3.3 sour 2.2.2.2……使用 2.2.2.2 作为源，测试与 3.3.3.3 的连通性。

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/69/84 ms

4.4. OSPF

4.4.1. OSPF基本配置

1、 OSPF 需要一个进程号，用来区分一个路由器上的 OSPF 进程。OSPF 也需要一个 area 号，在同一个 area 内的所有路由器都必须使用同一个 area 号，这样它们将用有一致的链路状态数据库。这里我们使用的 area 号为 100。
2、 实验拓扑：

3、 验证命令：

show ip protocols 命令用来显示关于整个路由的参数，过滤器以及网络的信息。

show ip route 命令显示路由器的路由表，表中包含了所有已知网络的列表和与其表中条目相关的子网。

show ip ospf interfaces 查看在那些接口上启用了 ospf 协议

show ip ospf neighbors 查看 ospf 的邻居表

show ip ospf topology 查看 ospf 的拓扑表

show ip ospf route 查看 ospf 学到的路由

4、 基本配置：

R2(config)#router ospf 1

R2(config-router)#network 2.2.2.0 0.0.0.255 area 100

R2(config-router)#network 26.26.26.0 0.0.0.255 area 100

R6(config)#router ospf 1

R6(config-router)#network 6.6. 6.0 0.0.0.255 area 100

R6(config-router)#network 26.26.26.0 0.0.0.255 area 100

R6(config-router)#network 36.36.36.0 0.0.0.255 area 100

R3(config)#router ospf 1

R3(config-router)#network 3.3.3.0 0.0.0.255 area 100

R3(config-router)#network 36.36.36.0 0.0.0.255 area 100

5、 验证：

配置过程中，应该会出现类似的提示 Dec 17 10:20:50.435: %OSPF-5-ADJCHG: Process 1, Nbr 6.6.6.6 on Serial0/3 from LOADING to FULL, Loading Done，该提示表示你当前配置的路由器与另一台 6.6.6.6 建立了邻居关系。通过命令 show ip ospf neighbours 可以查看邻居表，下表显示 R6 与 R2 和 R3 都建立了邻居关系。

R6#sh ip ospf neigh

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/-	00:00:34	36.36.36.3	Serial0/3
2.2.2.2	0	FULL/-	00:00:36	26.26.26.2	Serial0/2

通过 ping 命令测试 R2 与 R3 之间的联通性，也可以通过 show ip route 查看路由表，检查是否存在从 R2 去往 3.3.3.0 的路由。

R2#ping 3.3.3.3 source 2.2.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:

Packet sent with a source address of 2.2.2.2

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 16/37/76 ms

R2#sh ip route ospf

3.0.0.0/32 is subnetted, 1 subnets

O 3.3.3.3 [110/129] via 26.26.26.6, 00:20:20, Serial0/2

36.0.0.0/24 is subnetted, 1 subnets

O 36.36.36.0 [110/128] via 26.26.26.6, 00:20:20, Serial0/2

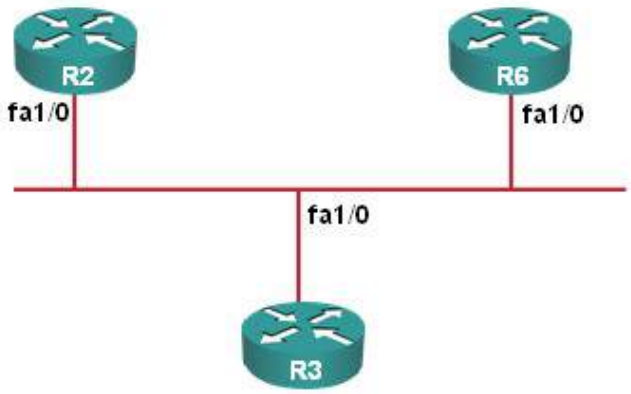
6.0.0.0/32 is subnetted, 1 subnets

O 6.6.6.6 [110/65] via 26.26.26.6, 00:20:20, Serial0/2

4.4.2. 广播多路访问链路上的OSPF

1、 OSPF 支持广播多路访问链路，且有 DR 的选举。

2、 实验拓扑：



3、 基本配置：

R2(config)#int fa1/0
R2(config-if)#ip add 123.1.1.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2……配置路由器的 ID
R2(config-router)#network 123.1.1.0 0.0.0.255 area 0

R3(config)#int fa1/0
R3(config-if)#ip add 123.1.1.3 255.255.255.0
R3(config-if)#no sh
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 123.1.1.0 0.0.0.255 area 0

R6(config)#int fa1/0
R6(config-if)#ip add 123.1.1.6 255.255.255.0
R6(config-if)#no sh
R6(config)#router ospf 1
R6(config-router)#router-id 6.6.6.6
R6(config-router)#network 123.1.1.0 0.0.0.255 area 0

4、 验证：

DR 选举的规则有：时间，首先启动的路由器被选为 DR；如果同时启动，或重新选举，则看接口优先级；前两者都相同，则看路由器的 ID，大者为 DR；DR 是非抢占的，除非认为重新选举。

通过在三台路由器上使用命令 show ip ospf neighbors 查看邻居，发现 R2 是 DR（最先启动），R3 是 BDR（第二启动），R6 是 DRother。

R2#sh ip ospf nei

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:39	123.1.1.3	FastEthernet1/0
6.6.6.6	1	FULL/DROTHER	00:00:39	123.1.1.6	FastEthernet1/0

下面我们通过更改 R6 的接口优先级（广播多路访问链路默认为 1），从而影响 OSPF DR 的选举结果。

R6(config)#int fa1/0
R6(config-if)#ip ospf priority 6……将接口优先级改为 6

此时还需要将 R2，R3 和 R6 的 OSPF 进程重启 clear ip ospf process，之后通过命令 show ip ospf neighbors 查看邻居，发现 R2 是 DRother，R3 是 BDR，R6 是 DR。

R6#sh ip ospf nei

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/DROTHER	00:00:33	123.1.1.2	FastEthernet1/0
3.3.3.3	1	FULL/BDR	00:00:32	123.1.1.3	FastEthernet1/0

4.4.3. 基于区域的OSPF简单口令验证

1、 实验拓扑：

2、 基本配置：

R2(config)#interface serial 0/2
R2(config-if)#ip address 26.26.26.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#intface loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.0
R2(config)#router ospf 1
R2(config-router)#network 2.2.2.0 0.0.0.255 area 0
R2(config-router)#network 26.26.26.0 0.0.0.255 area 0
R2(config-router)#area 0 authentication……区域 0 启用简单口令认证
R2(config-router)#exit
R2(config)#int s0/2
R2(config-if)#ip ospf authentication-key cisco……配置验证密码

R6(config)#interface serial 0/2
R6(config-if)#ip address 26.26.26.6 255.255.255.0
R6(config-if)#no shutdown
R6(config-if)#intface loopback 0
R6(config-if)#ip address 6.6.6.6 255.255.255.0
R6(config)#router ospf 1
R6(config-router)#network 6.6.6.0 0.0.0.255 area 0
R6(config-router)#network 26.26.26.0 0.0.0.255 area 0
R6(config-router)#area 0 authentication……区域 0 启用简单口令认证
R6(config-router)#exit
R6(config)#int s0/2
R6(config-if)#ip ospf authentication-key cisco……配置验证密码

3、 验证：

R6#sh ip ospf int s0/2

Serial0/2 is up, line protocol is up
Internet Address 26.26.26.6/24, Area 0
Process ID 1, Router ID 6.6.6.6, Network Type POINT_TO_POINT, Cost: 64
【output omitted】
Simple password authentication enabled……表明该接口启用了简单口令认证
R6#sh ip ospf
Routing Process "ospf 1" with ID 6.6.6.6
【output omitted】
Area BACKBONE(0)
Number of interfaces in this area is 2 (1 loopback)
Area has simple password authentication……表明区域 0 采用了简单口令认证
R6#debug ip ospf packet
*Mar 1 00:14:52.823: OSPF: rcv. v:2 t:1 l:48 rid:2.2.2.2
aid:0.0.0.0 chk:DC89 aut:1 auk: from Serial0/2

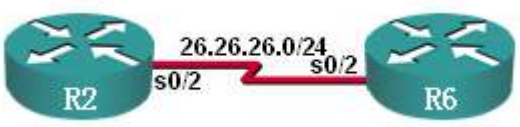
4.4.4. 基于区域的OSPF MD5认证

1、 该实验配置与上一个实验基本一致，只是认证方式不同，以下只给出不同的部分。
2、 MD5 认证配置：
R2(config-router)#area 0 authentication message-digest……区域 0 启用 MD5 认证
R2(config)#int s0/2
R2(config-if)#ip ospf message-digest-key 1 md5 cisco……配置验证 key ID 和密钥

R6(config-router)#area 0 authentication message-digest
R6(config)#int s0/2
R6(config-if)#ip ospf message-digest-key 1 md5 cisco
3、 验证：
R6#sh ip ospf int s0/2
Serial0/2 is up, line protocol is up
Internet Address 26.26.26.6/24, Area 0
Process ID 1, Router ID 6.6.6.6, Network Type POINT_TO_POINT, Cost: 64
【output omitted】
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
Message digest authentication enabled……启用 MD5 认证
Youngest key id is 1……使用密钥 ID 为 1 进行认证

4.4.5. default-information originate

1、 通过命令 default-information originate 可以向 OSPF 网络注入一条默认路由。该命令后可以加可选的“always”参数，如果不使用该参数，路由器上必须要存在一条默认路由，否则该命令不产生任何效果。如果使用该参数，无论路由器上是否存在默认你路由，路由器都将向 OSPF 区域注入一条默认路由。
2、 实验拓扑：



3、 基本配置：

```
R2(config)#interface serial 0/2
R2(config-if)#ip address 26.26.26.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#intface loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.0
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback0
R2(config)#router ospf 1
R2(config-router)#network 26.26.26.0 0.0.0.255 area 0
R2(config-router)#default-information originate

R6(config)#interface serial 0/2
R6(config-if)#ip address 26.26.26.6 255.255.255.0
R6(config-if)#no shutdown
R6(config-if)#intface loopback 0
R6(config-if)#ip address 6.6.6.6 255.255.255.0
R6(config)#router ospf 1
R6(config-router)#network 6.6.6.0 0.0.0.255 area 0
R6(config-router)#network 26.26.26.0 0.0.0.255 area 0
```

4、 验证：

```
R6#sh ip route
【output omitted】
Gateway of last resort is 26.26.26.2 to network 0.0.0.0

     6.0.0.0/24 is subnetted, 1 subnets
C       6.6.6.0 is directly connected, Loopback0
     26.0.0.0/24 is subnetted, 1 subnets
C       26.26.26.0 is directly connected, Serial0/2
O*E2 0.0.0.0/0 [110/1] via 26.26.26.2, 00:00:25, Serial0/2……R6 的路由表中出现了一条类型 2 的外部路由
R6#sh ip ospf data……R6 出现了一条类型 5 的 LSA
【output omitted】
                Type-5 AS External Link States

Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         2.2.2.2         278         0x80000001 0x00FEAB 1
```

4.4.6. 多区域OSPF基本配置

1、 OSPF 有两种类型的区域，骨干区域（只能是区域 0）和非骨干区域，当网络中定义了多个区域时，必须保证所有的非骨干区域要连接到骨干区域。

2、 非骨干区域的区域号可以自行定义，不一定非要连续。此实验中，非骨干区域使用 100。

3、 实验拓扑：

4、 基本配置：

```
R2(config)#router ospf 1
R2(config-router)#network 2.2.2.0 0.0.0.255 area 100
R2(config-router)#network 26.26.26.0 0.0.0.255 area 100

R6(config)#router ospf 1
R6(config-router)#network 6.6. 6.0 0.0.0.255 area 100
R6(config-router)#network 26.26.26.0 0.0.0.255 area 100
R6(config-router)#network 36.36.36.0 0.0.0.255 area 0

R3(config)#router ospf 1
R3(config-router)#network 3.3.3.0 0.0.0.255 area 0
R3(config-router)#network 36.36.36.0 0.0.0.255 area 0
```

5、 验证：

首先查看各路由器的路由表，

```
R2#sh ip route ospf
      3.0.0.0/32 is subnetted, 1 subnets
O IA     3.3.3.3 [110/129] via 26.26.26.6, 00:26:59, Serial0/2
      36.0.0.0/24 is subnetted, 1 subnets
O IA     36.36.36.0 [110/128] via 26.26.26.6, 00:27:33, Serial0/2
      6.0.0.0/32 is subnetted, 1 subnets
O        6.6.6.6 [110/65] via 26.26.26.6, 00:27:33, Serial0/2
```

备注：IA - OSPF inter area

然后测试 R2 和 R3 之间的连通性，

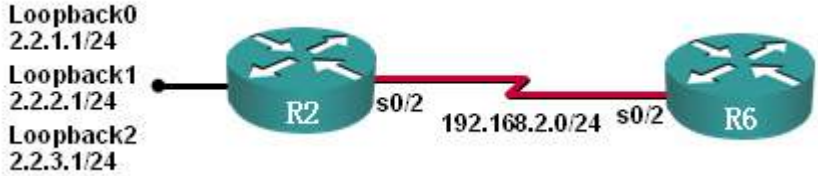
```
R2#ping 3.3.3.3 source 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/32/64 ms
```

4.4.7. OSPF手工总结

1、 OSPF 有两种汇总，一种是在 ABR 上汇总，另外一种是在 ASBR 上汇总。本实验中之介绍在 ABR 上汇总的方法，在 ASBR 上的汇总同学们自行设计完成。

2、 实验拓扑：



3、 基本配置：

```
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.1.1 255.255.255.0
R2(config-if)#int lo1
R2(config-if)#ip add 2.2.2.1 255.255.255.0
```

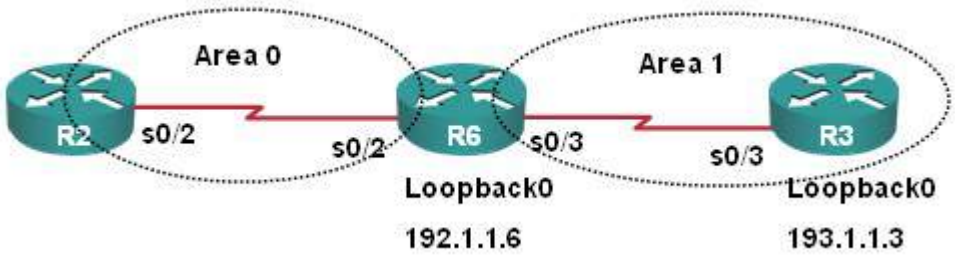
R2(config-if)#int l2
R2(config-if)#ip add 2.2.3.1 255.255.255.0
R2(config)#router ospf 1
R2(config-router)#route
R2(config-router)#router-id 1.1.1.1
R2(config-router)#net 2.2.1.0 0.0.0.255 area 1
R2(config-router)#net 2.2.2.0 0.0.0.255 area 1
R2(config-router)#net 2.2.3.0 0.0.0.255 area 1
R2(config-router)#net 192.168.2.0 0.0.0.255 area 0
R2(config-router)#area 1 range 2.2.0.0 255.255.0.0……将区域 1 中的三个网络汇总为 2.2.0.0/16

R6(config-router)#route
R6(config-router)#router-id 2.2.2.2
R6(config-router)#net 192.168.2.0 0.0.0.255 a 0

4、 验证：
执行汇总前，在 R6 的路由表中可以看到
R6#sh ip route
【output omitted】
2.0.0.0/32 is subnetted, 3 subnets
O IA 2.2.1.1 [110/65] via 192.168.2.1, 00:00:08, Serial0/2
O IA 2.2.3.1 [110/65] via 192.168.2.1, 00:00:08, Serial0/2
O IA 2.2.2.1 [110/65] via 192.168.2.1, 00:00:08, Serial0/2
执行汇总后
R6#sh ip route
【output omitted】
2.0.0.0/16 is subnetted, 1 subnets
O IA 2.2.0.0 [110/65] via 192.168.2.1, 00:00:03, Serial0/2

4.4.8. OSPF末节区域和完全末节区域

1、 末节区域和完全末节区域需要满足以下几个条件：区域只有一个出口；区域不需要作为需链路的过渡区；区域内没有 ASBR；区域不是主干区域。
2、 实验拓扑：



3、 基本配置：
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 26.26.26.0 0.0.0.255 area 0

在 R6 上创建回环接口，用于生成一条直连路由

R6(config)#router ospf 1
R6(config-router)#router-id 6.6.6.6
R6(config-router)#network 26.26.26.0 0.0.0.255 area 0
R6(config-router)#network 36.36.36.0 0.0.0.255 area 1
R6(config-router)#redistribute connected subnets……将直连路由重分布到 ospf
R6(config-router)#area 1 stub……配置区域 1 为末节区域
R6(config-router)#area 1 stub no-summary……配置区域 1 为完全末节区域

R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 36.36.36.0 0.0.0.255 area 1
R3(config-router)#area 1 stub
4、 验证：
R3#sh ip route ospf
26.0.0.0/24 is subnetted, 1 subnets
O IA 26.26.26.0 [110/128] via 36.36.36.6, 00:00:02, Serial0/3
O*IA 0.0.0.0/0 [110/65] via 36.36.36.6, 00:01:39, Serial0/3
以上输出表明 R6 重分布进来的回环接口所在网络 192.1.1.0 并没有在 R3 的路由表中出现，说明末节区域不接收类型 5 的 LSA，同时末节区域 1 的 ABR R6 自动向该区域内传播一条默认路由；末节区域可以接收区域间路由。
要配置区域 1 为完全末节区域，只需要在 R6 上执行命令 area 1 stub no-summary 即可，此时查看 R3 的路由表
R3#sh ip route ospf
O*IA 0.0.0.0/0 [110/65] via 36.36.36.6, 00:01:39, Serial0/3
以上输出说明，完全末节区域不接收外部路由和区域间路由，只有区域内的路由和一条 ABR（R6）向该区域注入的默认路由。
R6#sh ip ospf 1
【output omitted】
Area 1
Number of interfaces in this area is 2 (1 loopback)
It is a stub area, no summary LSA in this area
generates stub default route with cost 1……向 area 1 通告一条 cost=1 的默认路由

4.4.9. OSPF NSSA区域

1、 本实验在上一个实验的基础上进行，删除末节区域的配置即可。
2、 基本配置：
R3(config)#router ospf 1
R3(config-router)#area 1 nssa

R6(config)#router ospf 1
R6(config-router)#area 1 nssa
R6(config-router)#area 1 nssa no-summary
3、 验证：
R3#sh ip route ospf
O IA 26.26.26.0 [110/128] via 36.36.36.6, 00:00:33, Serial0/3
O N2 192.1.1.0/24 [110/20] via 36.36.36.6, 00:00:33, Serial0/3

以上输出发现，NSSA 可以传递区域间路由，也可以通过在 ABR（R6）上配置命令 area 1 nssa no-summary，此时 ABR 会向 NSSA 区域注入一条默认路由，如下所示

R3#sh ip route ospf

O N2 192.1.1.0/24 [110/20] via 36.36.36.6, 00:01:03, Serial0/3

O*IA 0.0.0.0/0 [110/65] via 36.36.36.6, 00:01:08, Serial0/3

5. LAN交换和无线篇

5.1. 交换机基本概念和基本配置

5.1.1. 交换机基本配置

1、 交换机与路由器的基本配置极其相似，以下给出部分配置;

基本安全配置

```
SW1>enable
SW1#config t
SW1(config)#enable password cisco
SW1(config)#service password-encryption
SW1(config)#line vty 0 4
SW1(config-line)#login
SW1(config-line)#password cisco1
SW1(config)#line con 0
SW1(config-line)#login
SW1(config-line)#password cisco2
```

接口配置

```
SW1(config)#interface fastethernet 0/1
SW1(config-if)#duplex [full half auto]
SW1(config-if)#speed [10 100 1000 auto]
```

管理地址配置

```
SW1(config)#interface vlan 1
SW1(config-if)#ip add 192.168.1.11 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#default-gateway 192.168.1.1
```

5.1.2. 使用GUI配置交换机

1、 使用浏览器或 CAN 软件配置交换机。

2、 本实验中采用浏览器配置，cisco catalyst 1900 支持 web 管理。

3、 基本配置：

首先给交换机配置管理地址，并确保你的 PC 机和该交换机之间的连通性。然后在浏览器地址栏输入你配置的管理地址，即可登陆。

```
1900#config t
1900(config)#ip add 192.168.1.1 255.255.255.0
1900(config-if)#no shutdown
```

5.1.3. 交换机端口安全

1、 配置交换机端口安全可以有效防止非法接入。

2、 交换机端口安全一般在接入层交换机上配置。

3、 配置静态安全 MAC 地址：

```
Switch(config)#interface fa0/1
Switch(config-if)#shutdown……关闭接口
Switch(config-if)#switch mode access
```

Switch(config-if)#switch port-security……启用端口安全
Switch(config-if)#switch port-security maximum 1……配置最大 MAC 条目
Switch(config-if)#switch port-security mac-address 0023.1123.3365……指定该接口只能学习的 MAC
Switch(config-if)#switch port-security violation shutdown……发生攻击时采取的动作，根据上面的配置，当该端口学习到两个 MAC 时将会自动 shutdown
Switch(config-if)#no shutdown

4、 配置动态安全 MAC 地址：

Switch(config)#interface fa0/1
Switch(config-if)#shutdown
Switch(config-if)#switch mode access
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security maximum 1
Switch(config-if)#switch port-security violation [shutdown protect restrict]
Switch(config-if)#no shutdown

当交换机的某个接口下连接有多个合法用户时，采用静态安全 MAC 显然有很大的工作量，不仅要查这些合法用户的 MAC，还需要手工绑定。在这里我们有一个简单的解决方法，采用粘滞安全 MAC 即可。

Switch(config-if)#switch port-security mac-address sticky

这条命令的另外一个好处是，当交换机学习到了所以的合法 MAC 后，你可以使用 copy running-config startup-config 将配置保存，重启交换机，该 MAC 表项依然存在。

5.1.4. 配置3550为DHCP服务器

Switch(config)#ip dhcp pool ccna……创建地址池 ccna
Switch(dhcp-config)#network 192.168.1.0 255.255.255.0……分配的 ip 地址
Switch(dhcp-config)#default-router 192.168.1.1……配置默认网关
Switch(dhcp-config)#exit
Switch(config)#ip dhcp execluded-address 192.168.1.1……排除地址
Switch(config)#interface fa0/1
Switch(config-if)#ip add 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown

5.1.5. 交换机的密码恢复

交换机的密码恢复与路由器稍有不同，下面给出 cisco catalyst 3550 的恢复方法。

1、 通过 console 线连接该交换机。
2、 关闭电源。
3、 打开电源，启动。并按住交换机背面的 mode 按键，当交换机端口 1X 上的 LED 熄灭后可以松开 Mode 按钮 1 到 2 秒.之后将显示一些指示信息:
4、 初始化 flash 文件系统:

switch#flash_init

5、 加载帮助文件:

switch#load_helper

6、 显示闪存里的内容:

switch#dir flash:

7、 重命名配置文件:

switch#rename flash:config.text flash:config.text.old

8、 启动系统,并且如果提示进入 setup 模式,输入 N:

switch#boot
Continue with the configuration dialog? [yes/no]: N
9、 进入特权模式,把配置文件名恢复为原始文件名:
Switch#rename flash:config.text.old flash:config.text
10、 把配置文件写进内存:
Switch#copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
11、 进入全局配置模式更改密码:
Switch(config)#enable secret {password}
12、 退出,并保存到 startup-config 文件里:
Switch(config)#copy running-config startup-config

5.1.6. 交换机的IOS恢复

交换机的 IOS 恢复与路由器类似。下面给出相应的步骤：
1、 将 PC 机与交换机通过 console 相连，用超级终端登陆到交换机上；
2、 由于交换机没有 IOS，因此执行下面的命令：
Switch:flash_ini
Switch:load_helper
3、 输入复制命令：
Switch:copy xmodem:flash:c2950-i6q412.mz.12.1-22.EA5a.bin
4、 传送完毕执行重启：
Switch:boot
另外，可以采用 TFTP 的方式传送，这种方式由同学们自行完成。

5.2. VLAN/Trunk和EtherChannel

5.2.1. 划分VLAN

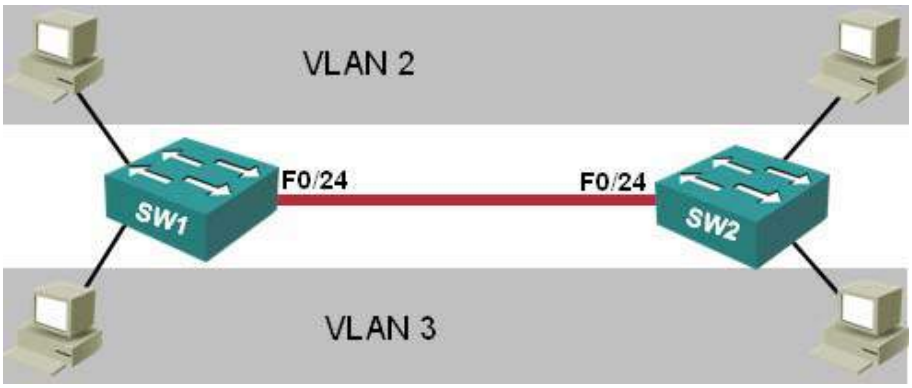
1、 划分 VLAN 有多种方法，在这里我们采用基于端口的划分方法。
2、 本实验只要一台交换机即可完成，这里采用 cisco catalyst 3550。
3、 基本配置：
SW(config)#vlan 10……创建 vlan 10
SW(config-vlan)#name ccna……命名 vlan 10 为 ccna
SW(config-vlan)#exit
SW(config)#int fa0/10
SW(config-if)#switchport mode access……将接口指定为 access 模式
SW(config-if)#switchport access vlan 10……将接口划入 vlan 10
创建其它 vlan 方法同上。
4、 验证：
通过 show vlan 可以查看当前交换机上存在的 vlan，以及哪些接口被划入到哪些特定的 vlan 中。在此要说明的是，默认时 cisco 交换机所有的接口都属于 vlan 1，并且 vlan 1 是不能删除、更改的。此外，还有一些特定的 vlan ID 给其他特定的 vlan，如 1002~1005。

5.2.2. Trunk配置

1、 Trunk 线路的特征是：一条 Trunk 线路上同时承载多个 vlan 的流量。如下图所示，SW1 和 SW2

之间的线路要同时传送 vlan 2 和 vlan 3 的流量，使得不同交换机上同一 vlan 内的用户可以相互访问。

2、 实验拓扑：



3、 基本配置：

首先在 SW1 和 SW2 上划分 vlan，此部分参考 vlan 划分实验。

Trunk 的基本配置

SW1(config)#interface fastethernet 0/24
SW1(config-if)#switchport trunk encapsulation dot1q……配置 802.1q 封装
SW1(config-if)#switchport mode trunk……配置接口为 trunk
SW1(config-if)#switchport trunk allowed vlan 1,2,3……配置 trunk 线路上允许通过的 vlan
SW1(config-if)#switchport trunk native vlan 1……配置 native vlan，dot1q 特有
SW1(config-if)#no shutdown

SW2(config)#interface fastethernet 0/24
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 1,2,3
SW2(config-if)#switchport trunk native vlan 1
SW2(config-if)#no shutdown

4、 验证：

通过 show int trunk fa0/24 查看 trunk 的相关状态，也可以通过 ping 测试 vlan2 和 vlan3 中两个用户的连通性。

5、 Trunk 还有另外一个类型的封装——ISL，交换机间链路，是 cisco 私有的协议，本实验中只给出 dot1q 的配置，ISL 的配置学员自行完成。

5.2.3. DTP配置

1、 DTP：动态 trunk 协议，通过相应的配置，链路两端可以协商成为 trunk。
2、 实验拓扑：与上个实验相同。
3、 DTP 协商规律：

State	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**

4、 基本配置：

SW1(config)#interface fastethernet 0/24
SW1(config-if)#switchport trunk encapsulation [isl dot1q]
SW1(config-if)#switchport mode [trunk | dynamic desirable | dynamic auto]
SW1(config-if)#switchport nonegotiate……配置接口为 nonegotiate
SW1(config-if)#no shutdown

SW2(config)#interface fastethernet 0/24
SW2(config-if)#switchport trunk encapsulation [isl dot1q]
SW2(config-if)#switchport mode [trunk | dynamic desirable | dynamic auto]
SW2(config-if)#switchport nonegotiate……配置接口为 nonegotiate
SW2(config-if)#no shutdown

5、 验证：

链路两端能否自动协商成功成为 trunk 链路，必须依照 DTP 协商规律表。配置完成后通过 sh dtp interface fa0/24 查看，是否成为 trunk。此外再通过 ping 进行测试同一 vlan 内用户的连通性。

5.2.4. EtherChannel配置

1、 Etherchannel：以太信道。配置 Etherchannel 可以有效增大链路带宽，并可以提供链路的冗余。基本思想是将多条物理线路捆绑成一条逻辑链路。以太信道有两种封装方式——pagp 和 lacp

2、 实验拓扑：

3、 基本配置：

SW1(config)#interface port-channel 1……创建以太信道 1
SW1(config)#interface range fa0/23 – 24
SW1(config-if)#channel-protocol pagp……采用 pagp
SW1(config-if)#channel-group 1 mode desiable……配置以太信道的模式
SW1(config-if)#switchport trunk encapsulation dot1q……封装以太信道中的物理接口
SW1(config-if)#switchport mode trunk……配置 trunk

SW2(config)#interface port-channel 1
SW2(config)#interface range fa0/23 – 24
SW2(config-if)#channel-protocol pagp
SW2(config-if)#channel-group 1 mode desiable
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk

4、 验证：

通过 show etherchannel summary 可以查看以太信道的组号，以及哪些接口被捆绑到以太信道。采用 lacp 的方式同学们自行完成。

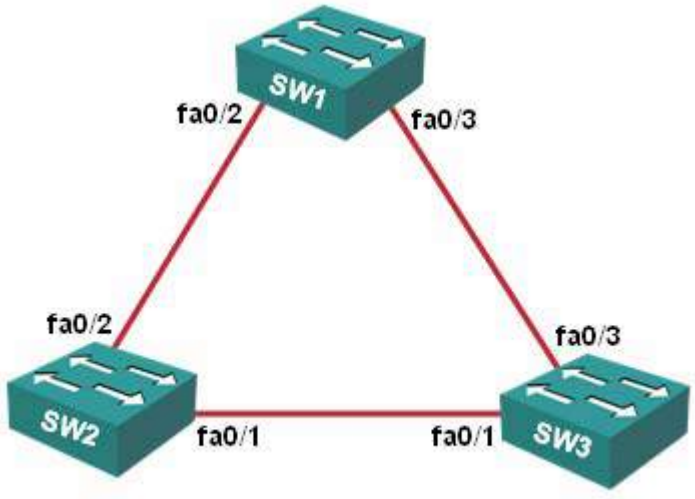
5.3. VTP

5.3.1. VTP配置

1、 VTP：vlan trunk protocol，可以帮助管理员减轻繁重的工作，使的交换机自动学习、同步关于 vlan 的变化信息。

2、 VTP 的三种模式：server、client 和 transprent。

3、 实验拓扑：



4、 基本配置：

将交换机 SW2 配置为 client

```
SW2(config)#vtp mode client
SW2(config)#vtp domain ccna
SW2(config)#vtp password chinaiplab
```

将交换机 SW3 配置为 transprent

```
SW3(config)#vtp mode transparent
SW3(config)#vtp domain ccna
SW3(config)#vtp password chinaiplab
```

将交换机 SW1 配置为 server

```
SW1(config)#vtp mode server
SW1(config)#vtp domain ccna
SW1(config)#vtp password chinaiplab
```

5、 验证：

首先在 SW1、SW2 和 SW3 上使用命令：show vtp status 查看 configuration revision 以及 vlan 的数目，并做相应记录。

在 SW1 上做如下更改，增加一个 vlan 100：SW1(config)#vlan 100，之后通过命令 show vtp status 查看三台交换机的 vtp 信息，发现 SW2 的 configuration revision 增加 1，vlan 的数目也增加 1，但是 SW3 没有发生任何变化。

在 SW2 上执行：

```
SW2(config)#interface fa0/2
SW2(config-if)#shutdown
SW2(config)#interface fa0/1
SW2(config-if)#no shutdown
```

并再次在 SW1 上增加一个 vlan 200，此时发现 SW2 的 configuration revision 再次增加 1，vlan 数目也再次增加 1，但是 SW3 仍然没有发生任何变化。

5.3.2. VLAN信息覆盖

1、 我们在课程中强调了，当你在原有的网络中加入一台新的交换机时，特别要注意新加入交换机的 vtp configuration revision 以及该交换机的 vtp domain，vtp password 等。

2、 当管理员将一台具有与原有网络相同 vtp domain，vtp password，vtp mode server，且 configuration revision 高于原有网络的交换机后，这台新加入的交换机将发送 vtp 信息，网络中的其它 client 交换机将接收、转发并同步该信息。后果是，client 交换机的 vlan 信息将与新加入的交换机一致，原有的正常的 vlan 信息将被打乱，导致网络的不可达。

3、 为了避免上述可能出现的问题，管理员向原有网络中添加新交换机之前必须做到：将新加入交换机的 vtp configuration revision 清零。

4、 清零的方法：

SW(config)#vtp mode transparent

SW(config)#vtp mode client

如果原有网络配置了 vtp domain name 和 vtp password，并该交换机也参与 vtp，只要在该交换机上增加配置 vtp domain 和 password。

5、 验证：

5.3.3. VTP修剪

1、 VTP 修剪的目的是减少不必要信息的发送而耗费网络带宽。

2、 VTP 修剪只需要在 Server 上启用。

3、 基本配置命令：SW(config)#vtp pruner

5.4. STP

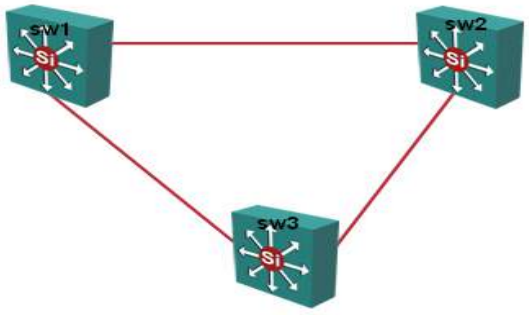
5.4.1. PVST配置

5.4.1.1. 实验目的

PVST：Per vlan STP，基于每个vlan都有一个生成树实例。在cisco catalyst 3550上，默认为pvst。

本实验的重点在于生成树根的选举、各端口状态的判断。

5.4.1.2. 实验拓扑：



5.4.1.3. 基本配置：

配置 VLAN 和 VTP，并使得三台交换机的 VTP 信息一致。

Cisco catalyst 3550 默认启用 PVST，因此无需配置。

5.4.1.4. 实验验证:

```
SW1#sh spanning-tree vlan 2

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    32770
              Address     000c.5866.2f80
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32770  (priority 32768 sys-id-ext 2)
              Address     000c.5866.2f80
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/19           Desg FWD 19        128.19   P2p
```

以上只给出了SW1的输出，通过比较三台交换机的输出，可以发现SW1为根桥，并且同时也是所以VLAN的生成树的根。可以通过命令SW2(config)#spanning-tree vlan 2 root primary将SW2指定为VLAN 2的根。

5.4.2. Portfast

5.4.2.1. 实验目的

Portfast是cisco对传统生成树的改进之一。传统生成树802.1d的收敛时间通常需要30~50秒。在这里要注意的是，对于启用了portfast特性的端口，只能连接终端（服务器或终端用户），这样该端口一旦有设备接入就立即转变为转发状态。从而避免类似DHCP Discover超时的问题。

5.4.2.2. 基本配置

配置portfast非常简单，有两种模式:

第一，在全局模式下SW(config)#spanning-tree portfast default，该命令可以全局启用交换机所以的access接口portfast特性;

第二，在接口模式下启用需要portfast特性的接口，命令为SW(config-if)#spanning-tree portfast。

5.4.3. RSTP

5.4.3.1. 实验目的

RSTP: 快速生成树（802.1w），实际上是把减少STP收敛时间的一些措施融合在STP协议中形成新的协议。RSTP收敛速度很快，有时甚至只需要几百毫秒。

5.4.3.2. 基本配置:

此实验的配置与上一个实验基本一致，只需要将三台交换机的生成树类型改为RSTP，cisco catalyst 3550只有RPVST，在三台交换机全局模式下执行命令为SW(config)#spanning-tree mode rapid-pvst，即可。验证命令与上个实验基本一致，在此不重复给出。

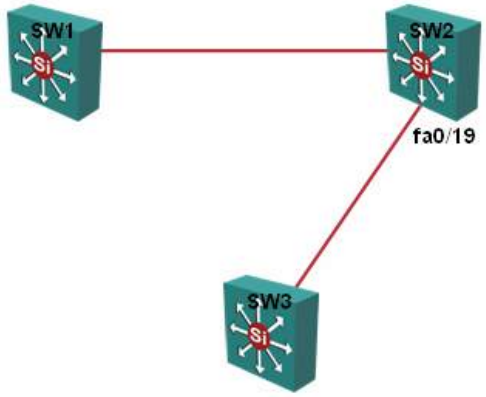
5.4.4. STP保护

5.4.4.1. 实验目的

本实验介绍root guard和bpdu guard。

Root guard和bpdu guard是在access端口上配置，其目的是防止用户非法接入其它交换机，从而造成stp重新收敛，甚至stp的根发生变化。

5.4.4.2. 实验拓扑:



5.4.4.3. 基本配置:

SW3是一台新交换机，且优先级为4096，SW1和SW2采用默认优先级。当没有配置任何防护措施时，SW3一旦接入网络，将会造成原有网络stp根的变化。此时的SW3不过是一个接入层交换机，并且性能一般，一旦它成为根，网络将会出现无法想象的后果。因此需要在SW1和SW2上的access接口配置root guard或bpdu guard。

首先介绍root guard的配置：例如在连接SW3的接口fa0/19上配置

SW2(config)#interface fa0/19

SW2(config-if)#spanning-tree guard root

配置root guard后，该接口将拒绝接收比现有根桥更优的bpdu。

下面介绍bpdu guard，同样也是在SW2的fa0/19上配置:

SW2(config)#interface fa0/19

SW2(config-if)#spanning-tree bpduguard enable

此时将交换机SW3与SW2连接起来，会发现SW2的fa0/19 down，通过命令SW2#show interface fa0/19

Fastethernet 0/19 is down,line protocol is down (err-disabled)，如果出现这种情况，要想使得fa0/19启用，首先必须移除bpdu源，然后在接口下执行shutdown、no shutdown命令。当然也可以通过配置相关命令，使其自动恢复SW2(config)#errdisabled recovery cause bpduguard，同时也可以指定恢复的时间SW2(config)#errdisabled recovery interval 60。

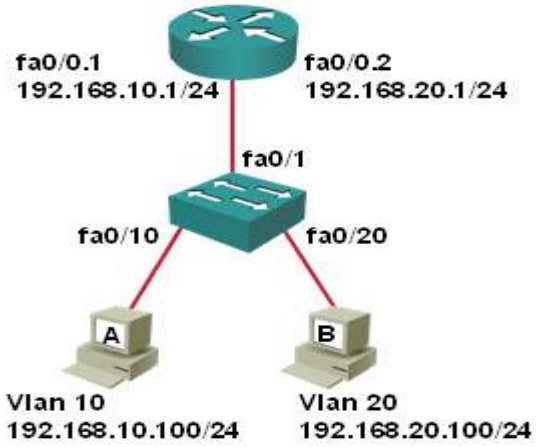
5.5. VLAN间路由

5.5.1. 单臂路由实现VLAN间路由

5.5.1.1. 实验目的

VLAN虽然给我们带来了很多好处，但是也带来了一些麻烦。默认时，不同vlan内的用户是不能相互访问的，为了解决这个问题，我们可以使用路由器。本实验主要介绍单臂路由的配置方法。

5.5.1.2. 实验拓扑:



5.5.1.3. 配置要点:

首先在交换机上划分vlan，并将相应的接口划入对应的vlan中。

SW(config)#vlan 10,20
SW(config)#interface fa0/10
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 10
SW(config)#interface fa0/20
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 20

配置交换机上的trunk：路由器和交换机之间的链路要承载多个vlan的流量，因此该链路一定要配置成trunk。

SW(config)#interface fa0/1
SW(config-if)#switchport trunk enacapsulation dot1q
SW(config-if)#switchport mode trunk
SW(config-if)#switchport trunk allowed vlan 1,10,20……定义允许通过的 vlan

路由器的配置：需要在路由器上创建子接口，分别对应vlan10和vlan20，且子接口的IP地址分别vlan10和vlan20中客户端的网关。

Router(config)#interface fa0/0
Router(config-if)#no shutdown
Router(config-if)#interface fa0/0.1
Router(config-subif)#ip add 192.168.10.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#interface fa0/0.2
Router(config-subif)#ip add 192.168.20.1 255.255.255.0
Router(config-subif)#encapsulation dot1q 20

5.5.1.4. 实验验证:

通过show ip route查看路由器的路由器，发现存在两条路由，分别到达192.168.10.0/24和192.168.20.0/24。然后在PCA上ping 192.168.2.100测试与PCB的通信是否正常。

C:\Documents and Settings\PCA>ping 192.168.20.100
Pinging 192.168.20.100 with 32 bytes of data:
Reply from 192.168.20.100: bytes=32 time=7ms TTL=64
Reply from 192.168.20.100: bytes=32 time=7ms TTL=64
Reply from 192.168.20.100: bytes=32 time=3ms TTL=64

Reply from 192.168.20.100: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

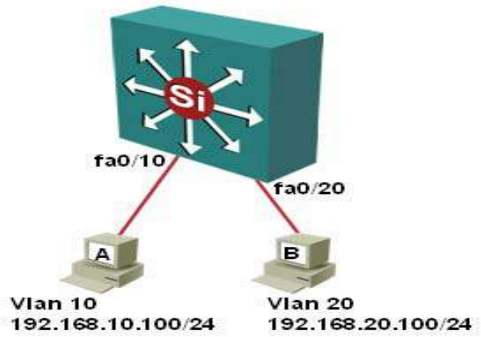
Minimum = 3ms, Maximum = 7ms, Average = 5ms

5.5.2. 三层交换实现VLAN间路由

5.5.2.1. 实验目的

为了实验vlan间的路由，还可以使用多层交换机。使用多层交换机主要是采用交换虚拟接口（SVI）来实现。

5.5.2.2. 实验拓扑:



5.5.2.3. 配置要点:

首先在交换机上划分 vlan，并将相应的接口划入对应的 vlan 中。

SW(config)#vlan 10,20

SW(config)#int fa0/10

SW(config-if)#switchport mode access

SW(config-if)#switchport access vlan 10

SW(config)#int fa0/20

SW(config-if)#switchport mode access

SW(config-if)#switchport access vlan 20

然后创建 SVI：相应 SVI 的 IP 地址将作为对应 vlan 中客户端的网关。

SW(config)#int vlan 10

SW(config-if)#ip add 192.168.10.1 255.255.255.0

SW(config-if)#no shutdown

SW(config-if)#int vlan 20

SW(config-if)#ip add 192.168.20.1 255.255.255.0

SW(config-if)#no shutdown

最后一定要在多层交换机上开启路由功能，否则无法实现 vlan 间的路由。

SW(config)#ip routing

5.5.2.4. 实验验证:

可以使用 show ip route 在交换机上查看路由表，可以发现两条路由，分别到达 192.168.10.0/24 和 192.168.20.0/24。然后在 PCA 上 ping 192.168.2.100 测试与 PCB 的通信是否正常。

C:\Documents and Settings\PCA>ping 192.168.20.100

Pinging 192.168.20.100 with 32 bytes of data:

Reply from 192.168.20.100: bytes=32 time=7ms TTL=64

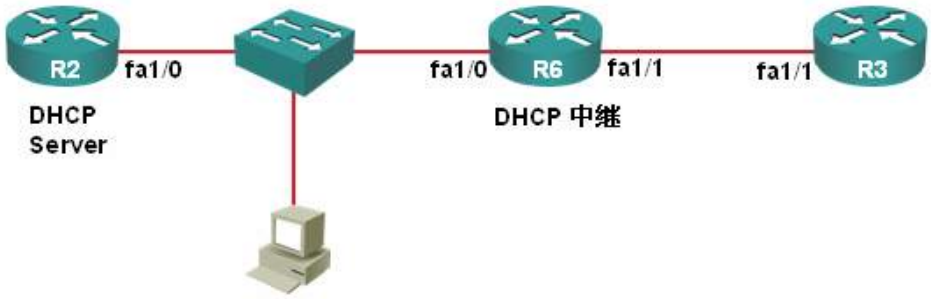
Reply from 192.168.20.100: bytes=32 time=7ms TTL=64
Reply from 192.168.20.100: bytes=32 time=3ms TTL=64
Reply from 192.168.20.100: bytes=32 time=3ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 7ms, Average = 5ms

5.5.3. 配置DHCP中继

5.5.3.1. 实验目的

客户端通过DHCP获得IP地址的过程中，客户端和服务器通过广播的方式交换，然而当客户端和服务器不在同一个网段时，客户端将无法正常获得IP地址。DHCP中继可以有效解决这一问题。

5.5.3.2. 实验拓扑:



R2 配置为 DHCP 服务器，R3 为 VLAN20 的一个用户，本机为 VLAN10 的一个用户，在 R6 上为 VLAN20 的用户配置 DHCP 中继代理。

5.5.3.3. 基本配置:

DHCP Server 配置：
R2(config)#int fa1/0
R2(config-if)#ip add 172.16.10.1 255.255.255.0
R2(config-if)#no sh

R2(config)#ip dhcp pool vlan10……配置 vlan 10 用户的地址池
R2(dhcp-config)#network 172.16.10.0 255.255.255.0
R2(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.5……定义排除地址

R2(config)#ip dhcp pool vlan20……配置 vlan 20 用户的地址池
R2(dhcp-config)#network 172.16.20.0 255.255.255.0
R2(dhcp-config)#default-router 172.16.20.1
R2(config)#ip dhcp excluded-address 172.16.20.1 172.16.20.5

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#net 172.16.10.0
R2(config-router)#no auto

R6 配置：

```
R6(config)#int fa1/0
R6(config-if)#ip add 172.16.10.2 255.255.255.0
R6(config-if)#no sh
R6(config)#int fa1/1
R6(config-if)#ip add 172.16.20.1 255.255.255.0
R6(config-if)#no sh
R6(config)#router rip
R6(config-router)#ver 2
R6(config-router)#net 172.16.10.0
R6(config-router)#net 172.16.20.0
R6(config-router)#no auto
```

R3 的配置：

```
R3(config)#no ip routing
R3(config)#int fa1/1
R3(config-if)#no sh
R3(config-if)#ip add dhcp
```

5.5.3.4. 实验验证:

本机获取的IP地址如下所示

```
C:\Documents and Settings\Administrator>ipconfig/renew
[output omitted]
        IP Address. . . . . . . . . . . . : 172.16.10.6
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.10.1
```

查看R3获取地址的情况

```
R3#
*Mar  1 00:26:15.707: %DHCP-6-ADDRESS_ASSIGN: Interface Fastethernet1/1 assigned DHCP
address 172.16.20.6, mask 255.255.255.0, hostname R3
R3#sh ip int bri | in up
Fastethernet1/1        172.16.20.6     YES DHCP        up              up
```

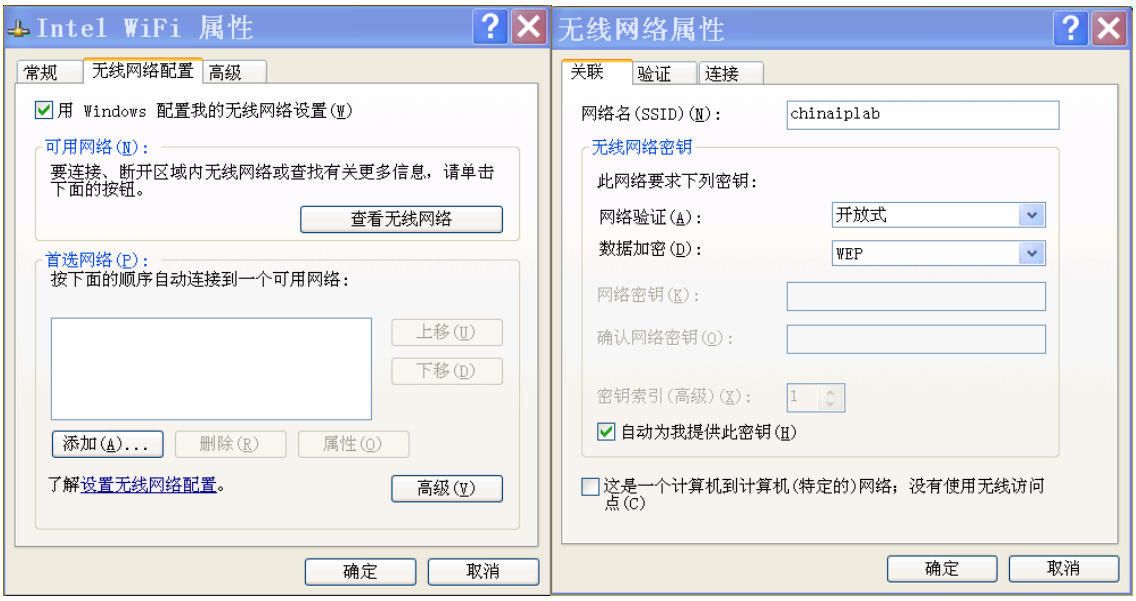
5.6. 无线

5.6.1. 无线网卡配置

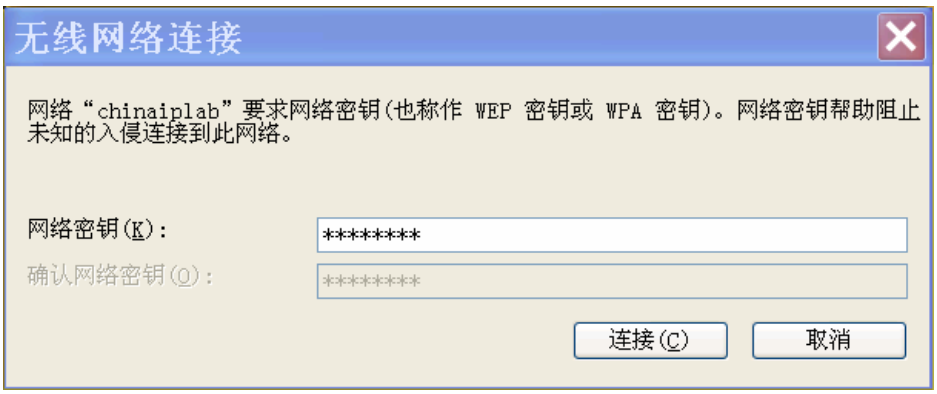
通过本实验可以掌握无线网卡的配置

在网络连接中双击“无线网络连接”，打开“无线网络连接”窗口，如下图所示

在上图中，单击右边的“更改高级设置”，打开“无线网络连接”窗口。如下左图所示:



选定**chianiplab**之后，单击“属性”，出现如上右图的属性窗口，填入必要的参数



在上图中单击“连接”按钮，就可以进行连接了。

成功连接后，在桌面的右下角会有一个无线连接图标。

5.6.2. LinkSys无线路由器配置

5.6.2.1. 位置选择

寻找最适宜的路由器位置。路由器的最佳位置通常是无线网络的中心，与所有无线设备位于一条直线上。如果使用可选外部天线，应立即对其进行调整，以便获得最佳性能。通常，天线放得越高，性能越好。

5.6.2.2. 设置路由器

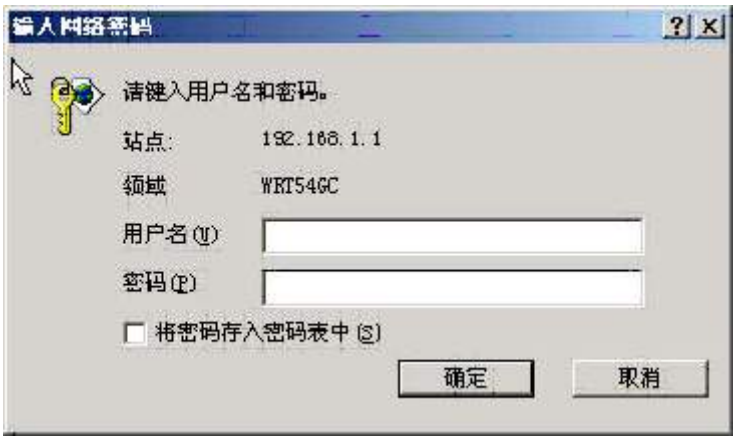
路由器支持基于 **Web** 的实用程序。

路由器的默省**IP** 地址为 **192.168.1.1**。所以首先把自己的电脑指定一个**IP**地址和路由器的**IP**地址在一个网段（如:**IP**地址: **192.168.1.100** 掩码**255.255.255.0**）。

1、要访问基于 **Web** 的实用程序，请启动 **Internet Explorer**或其它的浏览器。

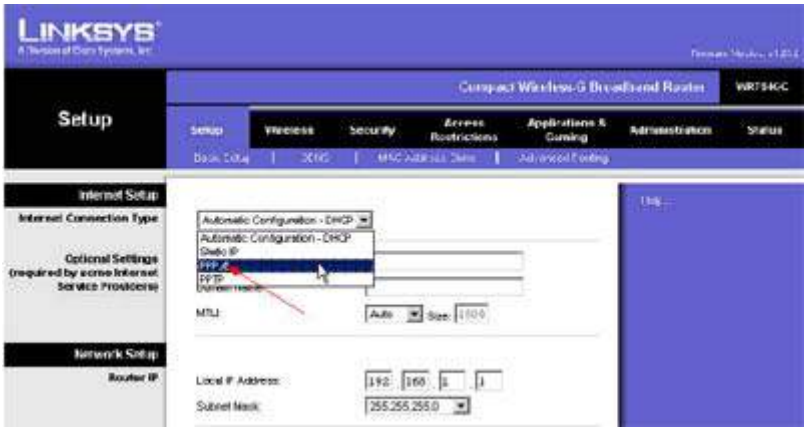
2、在地址栏输入路由器的地址**192.168.1.1**，然后按下 **Enter**。

3、在出现的口令请求页面。将用户名字段留空。使用默省口令**admin**。然后单击确定按钮。

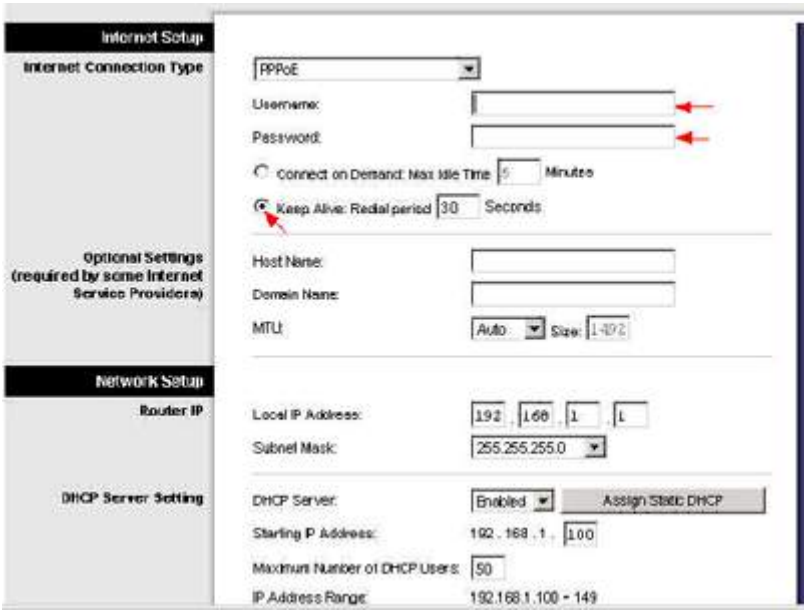


4、在出现的第一个屏幕显示**“setup”**选项卡。使用该选项卡可以更改路由器的常规设置。

5、在**Internet** 连接类型，从下拉菜单中选择 **ISP** 提供的 **Internet** 连接类型。一般使用**ADSL**的用户都选择**PPPOE**来上网。



6、如果是通过ADSL线路连接到 Internet，则必须启用 PPPoE。

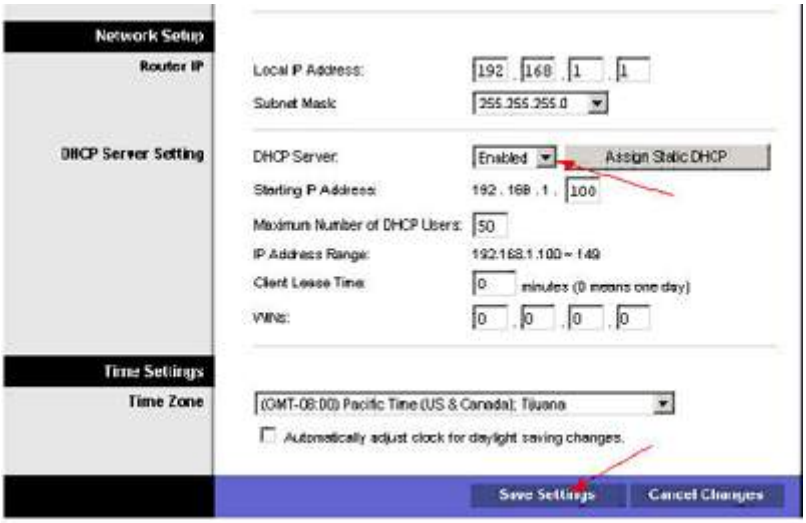


然后在用户名和口令分别输入申请宽带的用户名和口令

如果想让路由器连接后一直保持不断开，就选择**“keep alive..”** 选项。

5.6.2.3. 四、DHCP 服务器设置

DHCP 服务器出厂默认设置为启用 DHCP。此功能可以实现让电脑自动获取地址，并可通过路由器上因特网，所以一旦配置好了路由器，自己用的电脑不用指定地址，改为自动获取就可以上网了。



5.6.2.4. 状态检查

确保上面的设置都没有问题，点击页面的**“Save Setting”**按钮，路由器就会自动按上面的用户名和口令连接到因特网，一旦连接成功，点击**“Status”**菜单，就会显示出所有的系统信息，包括获取的公网地址等。

所有的配置都完毕，你就可以把自己的电脑改为自动获取地址，然后就开始上网吧。

6. 接入WAN篇

6.1. HDLC和PPP

6.1.1. HDLC和PPP封装

1、 HDLC：高级数据链路控制，cisco 设备在串行接口上默认采用该封装方式。PPP：点到点协议，是 IEEE 标准封装方式，用于连接不同厂商设备时。

2、 由于 HDLC 和 PPP 封装配置命令一致，故本实验只介绍 PPP 封装。

3、 实验拓扑：

4、 基本配置：

R2(config)#int s0/2
R2(config-if)#encapsulation ppp
此时在 R2 上会出现提示：%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down，因为此时 R6 是 HDLC，因此两端封装方式不一致，故接口 down。
R6(config)#int s0/2
R6(config-if)#encapsulation ppp
配置完上述命令后，R2 和 R6 都会出现类似的提示：%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to up

5、 验证：

通过 show run int [interface type|number]，show int [interface type|number]查看配置，最后通过 ping 来测试改变封装方式后的连通性。

```
R2#show run int s0/2
interface Serial0/2
 ip address 26.26.26.2 255.255.255.0
 encapsulation ppp

R2#sh int s0/2
Serial0/2 is up, line protocol is up
   Hardware is M4T
   Internet address is 26.26.26.2/24
   MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
       reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation PPP, LCP Open
R2#ping 26.26.26.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 26.26.26.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/47/80 ms
```

6.1.2. PAP验证

1、 将 R2 和 R6 相连的接口封装成 PPP，因此本实验可以在上个实验的基础上进行。

2、 启动 PAP 验证。PAP：Password Authentication Protocol，密码认证协议。

3、 基本配置：

```
R2(config)#int s0/2
R2(config-if)#ppp pap sent-username chinaiplab password cisco
R6(config)#int s0/2
R6(config-if)#ppp pap sent-username chinaiplab password cisco
```

配置完成后，R2 和 R6 上会出现提示：%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to up。

4、 验证：

```
R2#sh int s0/2
Serial0/2 is up, line protocol is up
  Hardware is M4T
  Internet address is 26.26.26.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
R2#ping 26.26.26.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 26.26.26.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/46/76 ms
```

PAP 验证采用明文方式，并且在两端协商过程中要发送用户名和口令，极易被别人窃取到（可以采用 wireshark 抓包查看用户名和口令）。

6.1.3. CHAP验证

1、 CHAP：挑战握手认证协议，该认证方式采取加密的方式，且协商过程中不发送密钥。

2、 基本配置：

```
R2(config)#username r2 password chinaiplab……建立本地认证数据库
R2(config)#int s0/2
R2(config-if)#encapsulation ppp
R2(config-if)#ppp chap hostname r6……认证用户名为 r6
R2(config-if)#ppp chap password chinaiplab……认证口令 chinaiplab

R6(config)#username r6 password chinaiplab
R6(config)#int s0/2
R6(config-if)#encapsulation ppp
R6(config-if)#ppp chap hostname r2
R6(config-if)#ppp chap password chinaiplab
```

该实验要注意的是，双方进行认证的口令必须一致。

3、 验证：

```
R2#sh int s0/2
Serial0/2 is up, line protocol is up
  Hardware is M4T
  Internet address is 26.26.26.2/24
```

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

R2#ping 26.26.26.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 26.26.26.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/46/76 ms

4、 当用户名、密码不正确时，认证将失败。例如将 R2 上的配置做如下更改，

R2(config)#no username r2 password cisco
R2(config)#username sajdls password 0 sjflsjf

此时 R2 和 R6 的通信没有出现问题，在这里需要注意的是，我们需要在 R2 或 R6 上使用命令 debug ppp authentication，然后将接口 shutdown 后 no shutdown，便可观察到认证失效的情况，

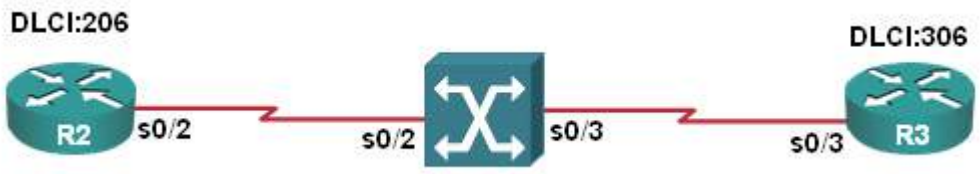
R2#debug ppp authentication
【output omitted】
R2(config)#int s0/2
R2(config-if)#shutdown
*Mar 1 01:07:49.871: %LINK-5-CHANGED: Interface Serial0/2, changed state to administratively down
*Mar 1 01:07:50.871: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down
R2(config-if)#no shutdown
*Mar 1 01:07:55.815: %LINK-3-UPDOWN: Interface Serial0/2, changed state to up
【output omitted】
*Mar 1 01:07:56.031: Se0/2 PPP: Sent CHAP LOGIN Request
*Mar 1 01:07:56.043: Se0/2 PPP: Received LOGIN Response FAIL
*Mar 1 01:07:56.047: Se0/2 CHAP: O FAILURE id 89 len 25 msg is "Authentication failed"

6.2. 帧中继

6.2.1. 把一台Cisco路由器配置为帧中继交换机

1、 不需要考虑传输差错问题，其中间节点只做帧的转发操作，不需要执行接收确认和请求重发等操作，差错控制和流量均交由高层端系统完成，大大缩短了节点的时延，提高了网内数据的传输速率。

2、 实验拓扑：



3、 基本配置：

R2(config)#int s0/2
R2(config-if)#no sh
R2(config-if)#ip add 192.1.1.2 255.255.255.0

R2(config-if)#encapsulation frame-relay

R6(config)#frame-relay switching……配置路由器为帧中继交换机
R6(config)#interface serial 0/2
R6(config-if)#encapsulation frame-relay……封装类型
R6(config-if)#frame-relay intf-type dce……配置接口类型
R6(config-if)#clock rate 64000
R6(config-if)#frame-relay route 206 int s0/3 306

R6(config-if)#int s0/3
R6(config-if)#encapsulation frame-relay
R6(config-if)#frame-relay intf-type dce
R6(config-if)#clock rate 64000
R6(config-if)#frame-relay route 306 int s0/2 206……从 s0/3 进入的 DLCI=306 的帧，通过 s0/2 口出站时 DLCI 号将交换为 206

R3(config)#int s0/3
R3(config-if)#no sh
R3(config-if)#ip add 192.1.1.3 255.255.255.0
R3(config-if)#encapsulation frame-relay

4、 验证：

在 R6 上查看路由表：

R6#sh fram route

Input Intf	Input Dlci	Output Intf	Output Dlci	Status
Serial0/2	206	Serial0/3	306	active
Serial0/3	306	Serial0/2	206	active

分别在 R2 和 R3 上测试 ping：

R2#ping 192.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/108/176 ms

6.2.2. 帧中继基本配置

1、 本实验在上一个实验的基础上进行。
2、 配置静态帧中继映射：
R2(config)#int s0/2
R2(config-if)#frame-relay interface-dlci 206
R2(config-if)#frame-relay map ip 192.1.1.2 206 broadcast……配置静态 FR 映射（如果没有上面三条命令，R2 ping 192.1.1.2 将无法成功。）

R3(config)#int s0/3
R3(config-if)#frame-relay interface-dlci 306
R3(config-if)#frame-relay map ip 192.1.1.3 306 broadcast
3、 验证：

R3#sh frame-relay map
Serial0/3 (up): ip 192.1.1.2 dlci 306(0x132,0x4C20), dynamic,
broadcast,, status defined, active……动态映射
Serial0/3 (up): ip 192.1.1.3 dlci 306(0x132,0x4C20), static,
CISCO, status defined, active……静态映射
R3#ping 192.1.1.2……与 R2 通信成功

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/97/192 ms
R3#ping 192.1.1.3……ping 自己的地址

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/184/332 ms

6.2.3. 帧中继网络上配置RIP

1、 本实验在帧中继基本配置的基础上进行。
2、 在 R2 和 R3 上分别建立一个 loopback 接口。
3、 基本配置：
R2(config)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#net 192.1.1.0
R2(config-router)#net 2.2.2.0
R2(config-router)#no auto

R3(config)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#net 192.1.1.0
R3(config-router)#net 3.3.3.0
R3(config-router)#no auto
4、 验证：
查看 R2 和 R3 的路由表，并测试 2.2.2.2 和 3.3.3.3 之间的连通性。
R3#sh ip route
【output omitted】

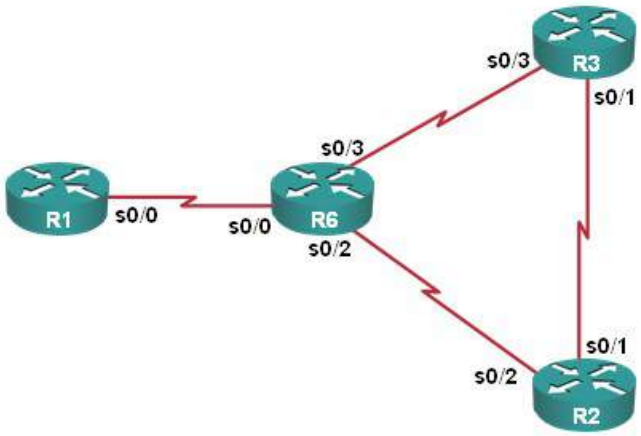
2.0.0.0/24 is subnetted, 1 subnets
R 2.2.2.0 [120/1] via 192.1.1.2, 00:00:07, Serial0/3
3.0.0.0/24 is subnetted, 1 subnets
C 3.3.3.0 is directly connected, Loopback0

C 192.1.1.0/24 is directly connected, Serial0/3
R3#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/97/160 ms

6.2.4. 帧中继点到多点模式下配置OSPF

1、 本实验只给出点到多点配置，帧中继的配置参考本章第一个实验。
2、 实验拓扑：



3、 基本配置：
配置 R6 为帧中继交换机
R6(config)#frame-relay switching
R6(config)#int s0/0
R6(config-if)#frame-relay intf-type dce
R6(config-if)#cl ra 64000
R6(config-if)#frame-relay route 102 int s0/2 201
R6(config-if)#frame-relay route 103 int s0/3 301
R6(config)#int s0/2
R6(config-if)#frame-relay intf-type dce
R6(config-if)#cl ra 64000
R6(config-if)#frame-relay route 201 int s0/0 102
R6(config)#int s0/3
R6(config-if)#frame-relay intf-type dce
R6(config-if)#cl ra 64000
R6(config-if)#frame-relay route 301 int s0/0 103

R1(config)#int s0/0
R1(config-if)#ip add 123.1.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#encapsulation frame-relay
R1(config-if)#fram interface-dlci 102
R1(config-if)#fram interface-dlci 103

```
R1(config-if)# ip ospf network point-to-multipoint
R1(config-if)#fram map ip 123.1.1.1 102 broadcast
R1(config-if)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#ip ospf network point-to-point
R1(config)#router ospf 1
R1(config-router)#net 1.1.1.0 0.0.0.255 area 0
R1(config-router)#net 123.1.1.0 0.0.0.255 area 0

R2(config)#int s0/2
R2(config-if)#ip add 123.1.1.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#encapsulation frame-relay
R2(config-if)#fram interface-dlci 201
R2(config-if)# ip ospf network point-to-multipoint
R2(config-if)#fram map ip 123.1.1.2 201 broadcast
R2(config)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config)#router ospf 1
R2(config-router)#net 2.2.2.0 0.0.0.255 area 0
R2(config-router)#net 123.1.1.0 0.0.0.255 a 0

R3(config)#int s0/3
R3(config-if)#ip add 123.1.1.3 255.255.255.0
R3 (config-if)#no sh
R3(config-if)#encapsulation frame-relay
R3(config-if)#fram interface-dlci 301
R3(config-if)#ip ospf net point-to-multipoint
R3(config-if)#fram map ip 123.1.1.3 301 broad
R3(config)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config)#router ospf 1
R3(config-router)#net  3.3.3.0 0.0.0.255 a 0
R3(config-router)#net 123.1.1.0 0.0.0.255 a 0
```

4、 验证：

```
R3#sh ip route ospf
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/65] via 123.1.1.1, 00:03:32, Serial0/3
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/129] via 123.1.1.1, 00:03:32, Serial0/3
      123.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        123.1.1.2/32 [110/128] via 123.1.1.1, 00:03:32, Serial0/3
O        123.1.1.1/32 [110/64] via 123.1.1.1, 00:03:32, Serial0/3
```

查看接口可以看到，网络类型为点到多点

```
R3#sh ip ospf int s0/3
Serial0/3 is up, line protocol is up
  Internet Address 123.1.1.3/24, Area 0
```

Process ID 1, Router ID 3.3.3.3, Network Type POINT_TO_MULTIPOINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,

6.2.5. 帧中继点到点子接口下配置OSPF

1、 本实验在帧中继基本配置的基础上进行。
2、 基本配置：

```
R2(config)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config)#int s0/2
R2(config-if)#ip ospf network point-to-point
R2(config-if)#exit
R2(config)#router ospf 1
R2(config-router)#network 2.2.2.0 0.0.0.255 area 1
R2(config-router)#network 192.1.1.0 0.0.0.255 area 0

R3(config)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config)#int s0/3
R3(config-if)#ip ospf network point-to-point
R3(config)#router ospf 1
R3(config-router)#network 192.1.1.0 0.0.0.255 area 0
R3(config-router)#network 3.3.3.0 0.0.0.255 area 2
```

3、 验证：
分别查看 R2 和 R3 的路由表，并测试 2.2.2.2 和 3.3.3.3 之间的连通性。

```
R3#sh ip route
【output omitted】

     2.0.0.0/32 is subnetted, 1 subnets
O IA    2.2.2.2 [110/65] via 192.1.1.2, 00:00:57, Serial0/3
     3.0.0.0/24 is subnetted, 1 subnets……
C       3.3.3.0 is directly connected, Loopback0
C    192.1.1.0/24 is directly connected, Serial0/3
R3#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/112/208 ms
```

6.3. 网络安全

6.3.1. 路由器的访问安全

1、 配置访问密码和 login 安全：

```
R2(config)#enable password chinaiplab……明文显示
R2(config)#enable secret ccna……密文显示
```

可以通过下面命令将明文密码加密成密文，

R2(config)#service password-encryption
R2#sh run
【output omitted】
enable secret 5 1TwLA$XWtAoAyuF96gua5qe.cdp1
enable password 7 0458030F0120455E051807
配置 Console 口登陆口令：
R2(config)#line console 0
R2(config-line)#login
% Login disabled on line 0, until 'password' is set
R2(config-line)#password chinaiplabccna……配置 Console 登陆口令
2、 配置用户登陆限制：
R2(config)#security authentication failure rate 5 log……配置用户连续登陆 5 次失败后，记录日志
R2(config)#login block-for 60 attempts 3 within 30……配置用户在 30 秒内连续 3 次登陆失败将进入 60 秒的安静期，在此期间任何人都无法登陆，但是可以通过以下命令指定某些合法用户可以登陆。
R2(config)#login quiet-mode access-class 10
R2(config)#access-list 10 permit 172.16.1.111……允许该 IP 地址的主机在静默期登陆
3、 配置提示信息：
R2(config)#banner motd #
Enter TEXT message. End with the character '#'.
Without authentication,shall not be visited!……配置提示信息
#
登陆时，可以看到此提示
Dec 20 10:01:59.351: %SYS-5-CONFIG_I: Configured from console by console
Without authentication,shall not be visited!
4、 配置 SSH：
R2(config)#clock timezone GMT +8……配置时区
R2#clock set 14:02:00 12 DEC 2009……配置路由器系统时间
R2(config)#ip domain-name cisco.com……配置域名
R2(config)#crypto key generate rsa……产生加密密钥
The name for the keys will be: R2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: ……密钥的长度
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

6.3.2. 路由器日志

1、 网络中有一台日志服务器，可以用一台安装了 syslog 软件的 PC 机构成，其 IP 地址为 172.16.1.1。
2、 配置路由器，使其与日志服务器之间能够通信，然后在路由器上配置如下命令
Router(config)#login 172.16.1.1……配置日志服务器的 IP 地址

6.3.3. 用SDM 配置路由器

1、 安装 SDM 时必须安装 Java 软件，在此推荐使用 SDMv24 和 Java jre-6u4-windows-i586-p。

2、 配置路由器，使得能够与 PC 机通信，配置如下：

Router(config)#ip http server……启用 http

Router(config)#ip http authentication local……启用本地认证

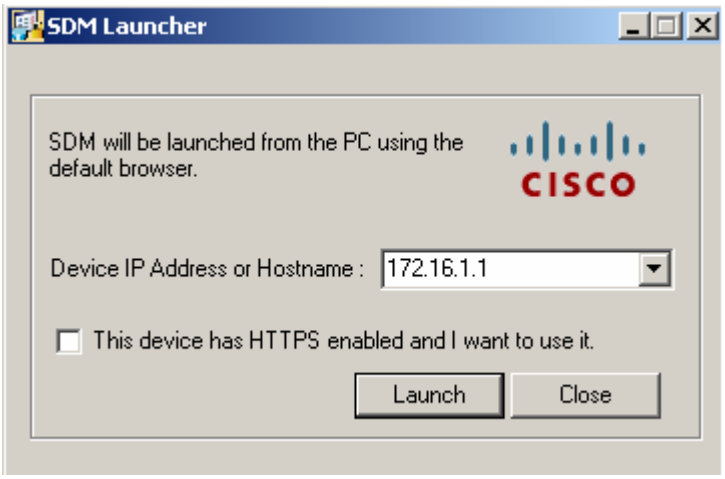
Router(config)#username ccna privilege 15 secret chinaiplab……配置本地用户名和口令

R2(config)#line vty 0 4

R2(config-line)#transport in all

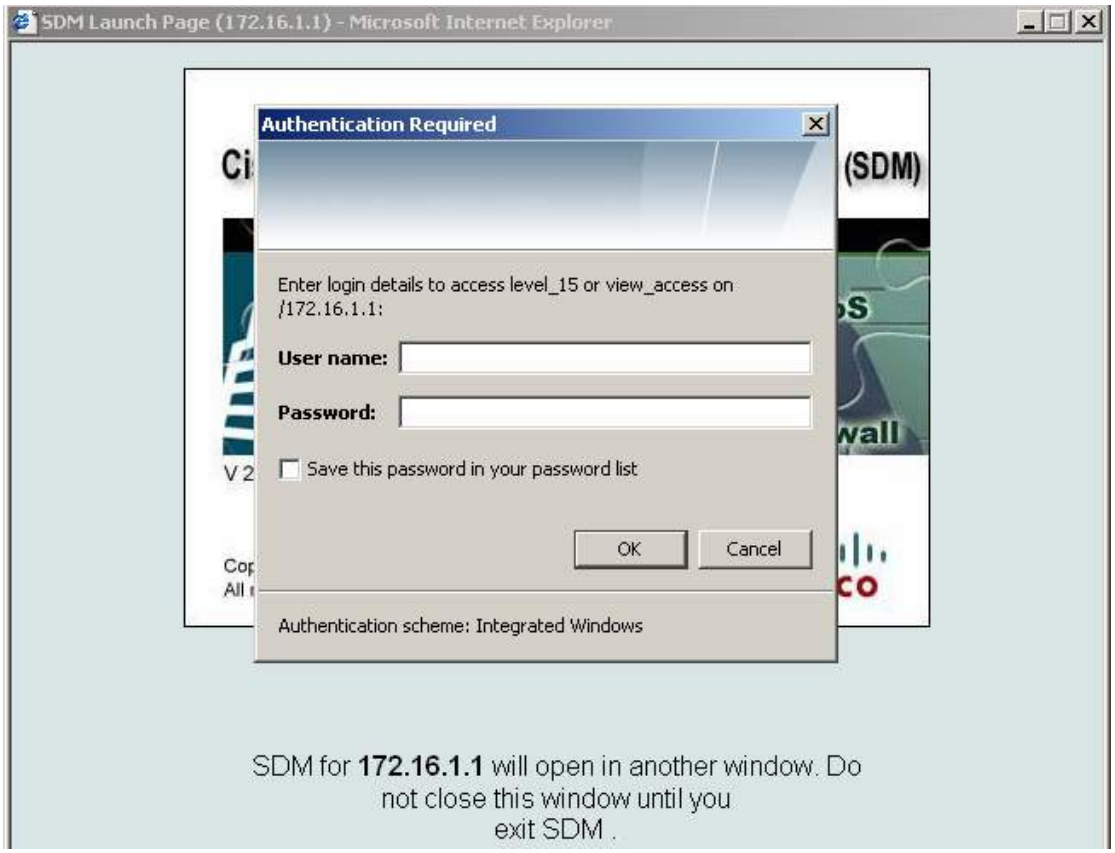
3、 使用 SDM 登陆

运行 SDM，输入路由器的 IP 地址，点击连接（Launch）

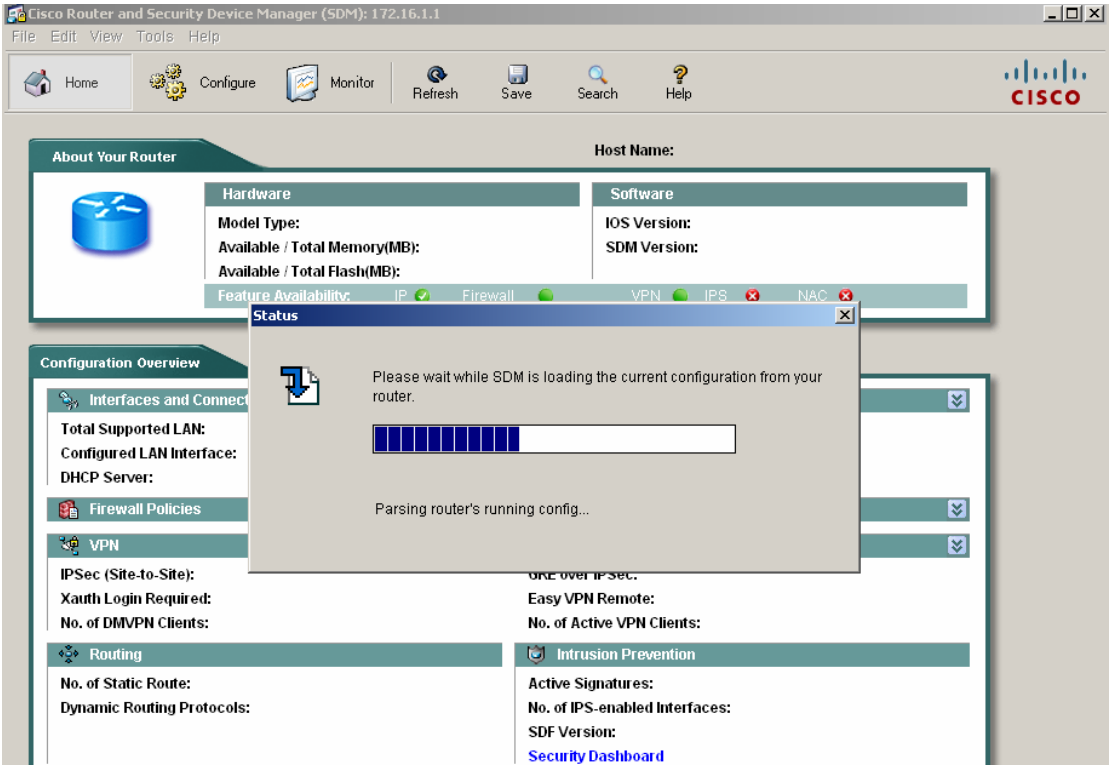


此时浏览器会提示无法显示，需要在浏览器设置中将“允许活动的内容在我的计算机上运行”，之后刷新，会出现登陆提示框

输入用户名 ccna，密码 chinaiplab，点击 OK



再次输入用户名和密码，点击 OK，即可登陆路由器



登陆路由器后，便可以使用 SDM 对该路由器进行配置，在此不详细介绍。

6.4. ACL

6.4.1. 标准ACL

1、 标准 ACL 只能对源进行过滤，编号范围 1-99。

2、 实验拓扑：

3、 基本配置：

R2(config)#router eigrp 1
R2(config-router)#net 2.2.2.0
R2(config-router)#net 26.26.26.0
R2(config-router)#no auto

R6(config)#router eigrp 1
R6(config-router)#net 6.6.6.0
R6(config-router)#net 26.26.26.0
R6(config-router)#no auto

使用 2.2.2.2 或 26.26.26.2 作为源，ping 6.6.6.6 都能通信。
R2#ping 6.6.6.6 source 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/27/88 ms
标准 ACL 一般配置在靠近目的的设备上，因此在 R6 上增加一条 ACL 用以拒绝 2.2.2.2 访问 R6，配置如下
R6(config)#access-list 1 deny 2.2.2.2
R6(config)#access-list 1 permit any……ACL 隐式拒绝一切，如果没有该命令将会拒绝所有通信
R6(config)#int s0/2
R6(config-if)#ip access-group 1 in……再接口上应用 ACL

4、 验证：

此时 2.2.2.2 将无法访问 R6
R2#ping 6.6.6.6 source 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
U.U.U
Success rate is 0 percent (0/5)
R2#ping 6.6.6.6 source 26.26.26.2……26.26.26.2 可以访问

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 26.26.26.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/36/104 ms

6.4.2. 扩展ACL

1、 扩展 ACL 可以同时对源和目的进行检查，还能够通过端口号进行限制。编号为 100-199，2000-2999。

2、 实验拓扑：与标准 ACL 一致。

3、 基本配置：在 R6 上配置扩展 ACL，用以拒绝 R2 的 Telnet 6.6.6.6，其它流量不受影响。另外，需要在 R6 上配置 vty 线路的口令。

R6(config)#access-list 110 deny tcp 26.26.26.0 0.0.0.255 host 6.6.6.6 eq telnet
R6(config)#access-list 110 permit ip any any
R6(config)#int s0/2
R6(config-if)#ip access-group 110 in……在接口下应用 ACL

4、 验证：

配置 ACL 前
R2#telnet 6.6.6.6
Trying 6.6.6.6 ... Open
User Access Verification
Password:
R6>
配置 ACL 后，并应用到接口上
R2#telnet 6.6.6.6
Trying 6.6.6.6 ...
% Destination unreachable; gateway or host down
但是其它流量不受影响，如 ping
R2#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!!

6.4.3. 基于时间ACL

1、 本实验要求 PC 机在 2009 年 12 月 20 日 14：00 到 15：00 之间可以 Telnet 访问路由器。

2、 实验拓扑：

3、 基本配置：

Router (config)#time-range ccna……定义时间范围
Router(config-time-range)#absolute start 14:00 20 Dec 2009 end 15:00 20 Dec 2009
Router (config)#access-list 110 permit tcp host 172.16.1.11 host 172.16.1.1 eq telnet log time-range ccna log
Router (config)#access-list 110 permit icmp any any
Router (config)#int e1/0
Router (config-if)#ip access-group 110 in

4、 验证：

通过 show access-list 110 查看当前 ACL 的状态，

Router#sh access-list 110

Extended IP access list 110

10 permit tcp host 172.16.1.11 host 172.16.1.1 eq telnet log time-range ccna (active)

20 permit icmp any any

此时可以正常通过 telnet 到路由器上，

User Access Verification

Password:……密码为 cisco

Router>

通过 clock set 更改路由器的时间，测试是否还能 telnet 到路由器上。

Router#clock set 16:00:00 20 December 2009 将路由器系统时间调整到 2009-12-20 下午 4 点，此时首先查看 ACL 的状态，

Router#sh access-list 110

Extended IP access list 110

10 permit tcp host 172.16.1.11 host 172.16.1.1 eq telnet log time-range ccna (inactive)

20 permit icmp any any

Telnet 已经不能成功登陆到路由器上了，

C:\Documents and Settings\Administrator>telnet 172.16.1.1

Connecting To 172.16.1.1...Could not open connection to the host, on port 23: Co

nnect failed

但是 ping 却不受影响，

C:\Documents and Settings\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time=80ms TTL=255

Reply from 172.16.1.1: bytes=32 time=63ms TTL=255

Reply from 172.16.1.1: bytes=32 time=101ms TTL=255

Reply from 172.16.1.1: bytes=32 time=85ms TTL=255

Ping statistics for 172.16.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 63ms, Maximum = 101ms, Average = 82ms

6.4.4. 动态ACL

1、 动态 ACL 是能够自动创建动态访问表项的访问列表。在动态访问表中，读者可以根据用户认证过程来创建特定的、临时的访问表项，一旦某个表项超时，就会自动从路由器中删除。

2、 实验拓扑：

在 R1 和 R2 上各有一 Loopback 接口模拟路由器背后的网络。现在 R1 如果需要访问 2.2.2.2/24，依据传统的访问列表如果处于路由器不可信任端的用户需要访问内部的资源，就必须永久性的在访问表中开启一个突破口以允许这些用户的流量进入可信任网络，但这个永久性的突破口也留下了安全隐患。通过动态访问列表能够提供更高的安全级别。

3、 基本配置：

```
R2(config)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#int s0/1
R2(config-if)#ip add 23.23.23.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 2.2.2.0
R2(config-router)#network 23.23.23.0
R2(config-router)#no auto

R3(config)#int l0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#int s0/1
R3(config-if)#ip add 23.23.23.3 255.255.255.0
R3(config-if)#no sh
R3(config-if)#exit
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 3.3.3.0
R3(config-router)#network 23.23.23.0
R3(config-router)#no auto

R3(config)#username test password cisco……创建本地用户名和口令
R3(config)#line vty 0 4
R3(config-line)#login local……启用本地认证
R3(config-line)#autocommand access-enable host time 1 …… 如果登陆成功自动执行命令 access-enable，使用 host 参数可以使动态表项替换认证主机的源 ip 地址（也就是 dynamic 命令中的源地址 any 会被动态表项的主机源 ip 地址替换），timeout 1 指空闲超时时间为 1 分钟
R3(config-line)#exit
R3(config)#ip access-list extended 100……创建命名访问控制列表
R3(config-ext-nacl)#permit tcp any host 23.23.23.3 eq telnet……允许任何主机 telnet 到 R3
R3(config-ext-nacl)#dynamic test timeout 3 permit ip any any……创建名为 test 的动态 ACL，绝对超时时间为 3 分钟（关于超时时间下面详述），表项允许所有流量通过。 此命令意为如果允许到达 R3 的 telnet 报文认证通过那么在动态的访问表项根据需要就会自动被创建
R3(config-ext-nacl)#exit
R3(config)#int s0/1
R3(config-if)#ip access-group 100 in
```

4、 验证：

```
R2#telnet 23.23.23.3
Trying 23.23.23.3 ... Open
```

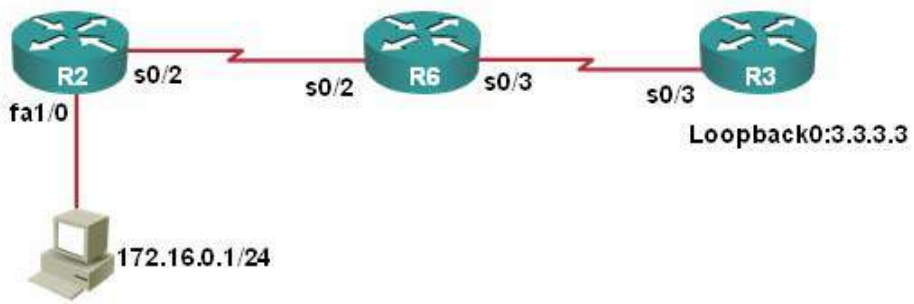
User Access Verification

Username: test
Password:
[Connection to 23.23.23.3 closed by foreign host]
R2#……telnet 很快被关闭
telnet 之前，在 R3 上查看 ACL
R3#sh access-lists
Extended IP access list 100
10 permit tcp any host 23.23.23.3 eq telnet
20 Dynamic test permit ip any any
telnet 之后，在 R3 上查看 ACL
R3#sh access-lists
Extended IP access list 100
10 permit tcp any host 23.23.23.3 eq telnet (72 matches)
20 Dynamic test permit ip any any
permit ip host 23.23.23.2 any……出现动态 ACL
telnet 之前，R3 的路由表
R3#sh ip route
【output omitted】
3.0.0.0/24 is subnetted, 1 subnets
C 3.3.3.0 is directly connected, Loopback0
23.0.0.0/24 is subnetted, 1 subnets
C 23.23.23.0 is directly connected, Serial0/1
没有学习到 R2 通告的 RIP 路由
telnet 之后，R3 的路由表
R3#sh ip route rip
2.0.0.0/24 is subnetted, 1 subnets
R 2.2.2.0 [120/1] via 23.23.23.2, 00:00:01, Serial0/1

6.4.5. 自反ACL

1、 本实验要求内网主机可以主动访问外网，但是外网主机不能主动访问内网，从而有效保护内网。

2、 实验拓扑：



3、 基本配置：

R2(config)#int fa1/0
R2(config-if)#ip add 172.16.0.11 255.255.0.0

R2(config-if)#no sh
R2(config)#int s0/2
R2(config-if)#ip add 26.26.26.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 26.26.26.6

R6(config)#int s0/2
R6(config-if)#ip add 26.26.26.6 255.255.255.0
R6(config-if)#no sh
R6(config-if)#int s0/3
R6(config-if)#ip add 36.36.36.6 255.255.255.0
R6(config-if)#no sh
R6(config-if)#exit
R6(config)#ip route 172.16.0.0 255.255.0.0 26.26.26.2
R6(config)#ip route 3.3.3.0 255.255.255.0 36.36.36.3

R3(config)#int s0/3
R3(config-if)#ip add 36.36.36.3 255.255.255.0
R3(config-if)#no sh
R3(config-if)#int loo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 36.36.36.6
通过以上配置，PC 可以与外网通信：
C:\Documents and Settings\Administrator>ping 3.3.3.3

Pinging 3.3.3.3 with 32 bytes of data:

Reply from 3.3.3.3: bytes=32 time=179ms TTL=253
Reply from 3.3.3.3: bytes=32 time=173ms TTL=253
Reply from 3.3.3.3: bytes=32 time=85ms TTL=253
Reply from 3.3.3.3: bytes=32 time=85ms TTL=253

Ping statistics for 3.3.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 85ms, Maximum = 179ms, Average = 130ms
R6 是内网和外网的边界，在 R6 上配置自反 ACL：
R6(config)#ip reflexive-list timeout 600……配置临时性访问条目的生存时间
R6(config)#ip access-list extended aclout……ACL 名称为 aclout
R6(config-ext-nacl)#permit tcp any any reflect ccna……创建自反 ACL（名称为 ccna）表项
R6(config-ext-nacl)#permit udp any any reflect ccna
R6(config-ext-nacl)#permit icmp any any reflect ccna
R6(config)#ip access-list extended aclin
R6(config-ext-nacl)#evaluate ccna……评估反射列表
R6(config-ext-nacl)#exit

R6(config)#int s0/3
R6(config-if)#ip access-group aclout out
R6(config-if)#ip access-group aclin in

4、 验证：

在 R3 上开启 telnet 服务，在 PC 机上 ping 和 telnetR3 的环回地址都能成功，查看 R6 上的 ACL：

R6#sh access-lists
Extended IP access list aclin
    10 evaluate ccna
Extended IP access list aclout
    10 permit tcp any any reflect ccna (20 matches)
    20 permit udp any any reflect ccna
    30 permit icmp any any reflect ccna
Reflexive IP access list ccna……IP 反射列表
     permit tcp host 3.3.3.3 eq telnet host 172.16.0.1 eq 1200 (38 matches) (time left 483)

以上两条输出说在从内部到外部 telnet 流量和 ping 流量经过时，临时自动产生一条 ACL 表项。

然后，在 R2 上开启 telnet 服务，从 R3 测试到 R2 的 ping 和 telnet：

R3#telnet 172.16.0.11
Trying 172.16.0.11 ...
% Destination unreachable; gateway or host down

R3#ping 172.16.0.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)

R6 上的 ACL 列表中也没有产生临时的 ACL 表项：

R6#sh access-lists
Extended IP access list aclin
    10 evaluate ccna
Extended IP access list aclout
    10 permit tcp any any reflect ccna
    20 permit udp any any reflect ccna
    30 permit icmp any any reflect ccna
Reflexive IP access list ccna
     permit icmp host 3.3.3.3 host 172.16.0.1 (time left 405)
R6#sh access-lists
Extended IP access list aclin
    10 evaluate ccna
Extended IP access list aclout
    10 permit tcp any any reflect ccna
    20 permit udp any any reflect ccna
    30 permit icmp any any reflect ccna
Reflexive IP access list ccna……IP 反射列表

以上输出说明自反 ACL 在有流量从外部发起时，不会临时自动产生一条 ACL 表项，所以不能访问成功。

6.5. IP编址服务

6.5.1. 在路由器上配置DHCP服务

1、 DHCP：Dynamips Host Configuration Protocol，动态主机配置协议。其功能是向客户端动态分配 IP 地址等参数。

2、 该实验要在 cisco 340 上配置 DHCP，并能成功向其它客户端动态分配 IP 地址，掩码，网关等参数。

3、 实验环境说明：该实验需要一台 cisco 3640 路由器和一台 PC 机，PC 机通过交叉线连接到路由器的以太接口。

4、 基本配置：将 R2 配置为 DHCP 服务器

```
R2(config)#int e1/0
R2(config-if)#ip add 192.168.1.1 255.255.255.0
R2(config-if)#no sh
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 192.168.1.2
R2(dhcp-config)#exit
R2(config)#ip dhcp excluded-address 192.168.1.1……排除地址
R2(config)#ip dhcp excluded-address 192.168.1.2
```

5、 验证：

将 PC 机的 TCP/IP 属性设置为自动获取 IP 地址，在 PC 机上查看相关 TCP/IP 属性，

```
C:\Documents and Settings\Administrator>ipconfig/all
【output omitted】
Physical Address. . . . . : 00-C0-CA-51-13-9B
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.2
```

6.5.2. 静态NAT配置

1、 NAT：Network Address Translation，网络地址转换。其功能是将内部地址转换为外部某个或某些地址，实现多人通过某个或某些 IP 地址连接到 Internet。

2、 实验环境说明：用一台 PC 机当做内网主机，配置 IP 地址为 192.168.0.100，掩码为 255.255.255.0，默认网关为路由器的内网地址 192.168.0.1；另外一台 PC 机模拟 Baidu 的主机，配置 IP 地址为 202.102.22.43，掩码为 255.255.255.0，默认网关为路由器的外网地址 202.102.22.1。

3、 基本配置：

首先将两台 PC 机的 TCP/IP 属性安装实验环境说明进行配置。

然后配置用于 NAT 的路由器。

```
R2(config)#int e0/1
R2(config-if)#ip add 192.168.0.1 255.255.255.0……配置内网接口的 IP 地址和掩码
R2(config-if)#ip nat inside……内网接口配置为 NAT 转换的入接口
R2(config-if)#no shutdown
```

R2(config-if)#int e0/2
R2(config-if)#ip add 202.102.22.1 255.255.255.0……配置外网接口的 IP 地址和掩码
R2r(config-if)#ip nat outside……外网接口配置为 NAT 转换的出接口
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ip nat inside source static 192.168.0.100 202.102.22.1 …… 将 192.168.0.1 转换成 202.102.22.1
4、 验证：
R2#sh ip nat trans……查看路由器的 NAT 转换表

Pro	Inside global	Inside local	Outside local	Outside global
---	202.102.22.1	192.168.0.1	---	---

在内网主机上测试：
C:\Documents and Settings\Administrator>ping 202.102.22.43

Pinging 202.102.22.43 with 32 bytes of data:

Reply from 202.102.22.43: bytes=32 time<1ms TTL=128
Reply from 202.102.22.43: bytes=32 time<1ms TTL=128
Reply from 202.102.22.43: bytes=32 time<1ms TTL=128
Reply from 202.102.22.43: bytes=32 time<1ms TTL=128

Ping statistics for 202.102.22.43:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

6.5.3. 动态NAT配置

1、 动态 NAT 的基本配置与静态 NAT 大致一样，只需要在 R2 上做如下更改。
2、 基本配置：
R2(config)#ip nat inside source static 192.168.0.100 202.102.22.1……删除原先的静态转换
R2(config)#ip nat pool NAT 202.102.22.1 202.102.22.10 netmask 255.255.255.0……配置一个动态地址池 NAT，池中有 202.102.22.1 到 202.102.22.10 共 10 个地址
R2(config)#access-list 1 permit 192.168.1.0 0.0.0.255……配置允许动态 NAT 转换的内部地址
R2(config)#ip nat inside source list 1 NAT……配置动态 NAT 映射，将 NAT 地址池与 ACL 绑定
3、 验证：
在内网主机上测试：
C:\Documents and Settings\Administrator>ping 202.102.22.43

Pinging 202.102.22.43 with 32 bytes of data:

Reply from 202.102.22.43: bytes=32 time<1ms TTL=128
Reply from 202.102.22.43: bytes=32 time<1ms TTL=128
Reply from 202.102.22.43: bytes=32 time<1ms TTL=128
Reply from 202.102.22.43: bytes=32 time<1ms TTL=128

Ping statistics for 202.102.22.43:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

6.5.4. NAT过载配置

1、 保留上个实验的配置，只需要 将 R2 的配置修改为：
R2(config)#ip nat inside source list 1 NAT overload……配置 NAT 过载
如果需要转换的主机数量不多，也可以直接在 outside 接口配置 NAT 过载，不需要定义地址池，命令如下：
R2(config)#ip nat inside source list 1 interface s0/2 overloaad
2、 验证：
通过命令 show ip nat translations，show ip nat statistics 查看配置，在此不再赘述。

6.5.5. IPv6静态路由配置

1、 IPv6 静态路由配置方法与 IPv4 一样。
2、 基本配置：
R2(config)#ipv6 unicast-routing ……启用 IPv6 路由
R2(config)#int loopback0
R2(config-if)#ipv6 address 2010:2222::2/64……配置 IPv6 地址
R2(config-if)#int s0/2
R2(config-if)#ipv6 add 2009:2626::2/64
R2(config-if)#no shut
R2(config)#ipv route::/0 s0/2……配置 IPv6 默认路由

R6(config)#ipv6 unicast-routing
R6(config)#int loopback0
R6(config-if)#ipv6 address 2010:6666::6/64
R6(config-if)#int s0/2
R6(config-if)#ipv6 add 2009:2626::6/64
R6(config-if)#no shut
R6(config)#ipv route 2010:2222::/64 s0/2……配置 IPv6 静态路由

3、 验证：
R6#ping ipv 2010:2222::2……注意与 IPv4 中 ping 的区别

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2010:2222::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/17/32 ms
查看 IPv6 路由表中的路由条目：
R2#sh ipv6 static
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via interface Serial0/2, distance 1

6.5.6. IPv6的RIPng配置

1、 RIPng：RIP Next Generation，RIP 下一代。与 RIP 版本 1 和版本 2 不同的是，RIPng 能支持 IPv6。

2、 实验拓扑：

3、 基本配置：

```
R2(config)#ipv6 unicast-routing
R2(config)#ipv6 router rip cisco……cisco 表示 RIPng 进程名
R2(config)#int s0/2
R2(config-if)#ipv6 address 2011:1111::2/64
R2(config-if)#ipv6 rip cisco enable
R2(config-if)#no shutdown

R6(config)#ipv6 unicast-routing
R6(config)#ipv6 router rip cisco
R6(config)#int s0/2
R6(config-if)#ipv6 address 2011:1111::6/64
R6(config-if)#ipv6 rip cisco enable
R6(config-if)#no shutdown
R6(config)#int s0/3
R6(config-if)#ipv6 address 2022:2222::6/64
R6(config-if)#ipv6 rip cisco enable
R6(config-if)#no shutdown

R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router rip cisco
R3(config)#int s0/3
R3(config-if)#ipv6 address 2022:2222::3/64
R3(config-if)#ipv6 rip cisco enable
R3(config-if)#no shutdown
```

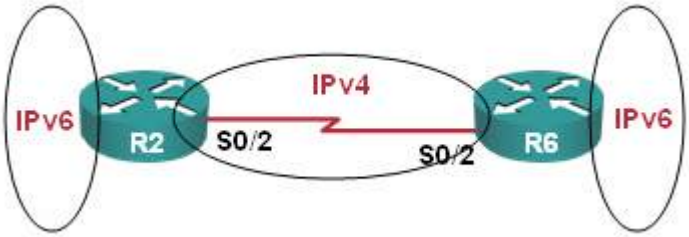
4、 验证：

验证命令有 show ipv6 route，show ipv6 rip database,也可以通过 ping 进行测试。

6.5.7. IPv6隧道配置

1、 IPv6 隧道是在 IPv4 向 IPv6 迁移过程中用到的一种技术，主要是解决 IPv4 和 IPv6 同时存在且通信不受影响的任务。

2、 实验拓扑：



3、 基本配置：

```
R2(config)#ipv6 unicast-routing
R2(config)#int loopback 0
R2(config-if)#ipv6 address 2011:2222::2/64
R2(config-if)#int s0/2
R2(config-if)#ip add 26.26.26.2 255.255.255.0
R2(config-if)#no shutdown

R6(config)#ipv6 unicast-routing
R6(config)#int loopback 0
R6(config-if)#ipv6 address 2011:6666::6/64
R6(config-if)#int s0/2
R6(config-if)#ip add 26.26.26.6 255.255.255.0
R6(config-if)#no shutdown
```

4、 验证：

在R2上ping ipv6 2011:6666::

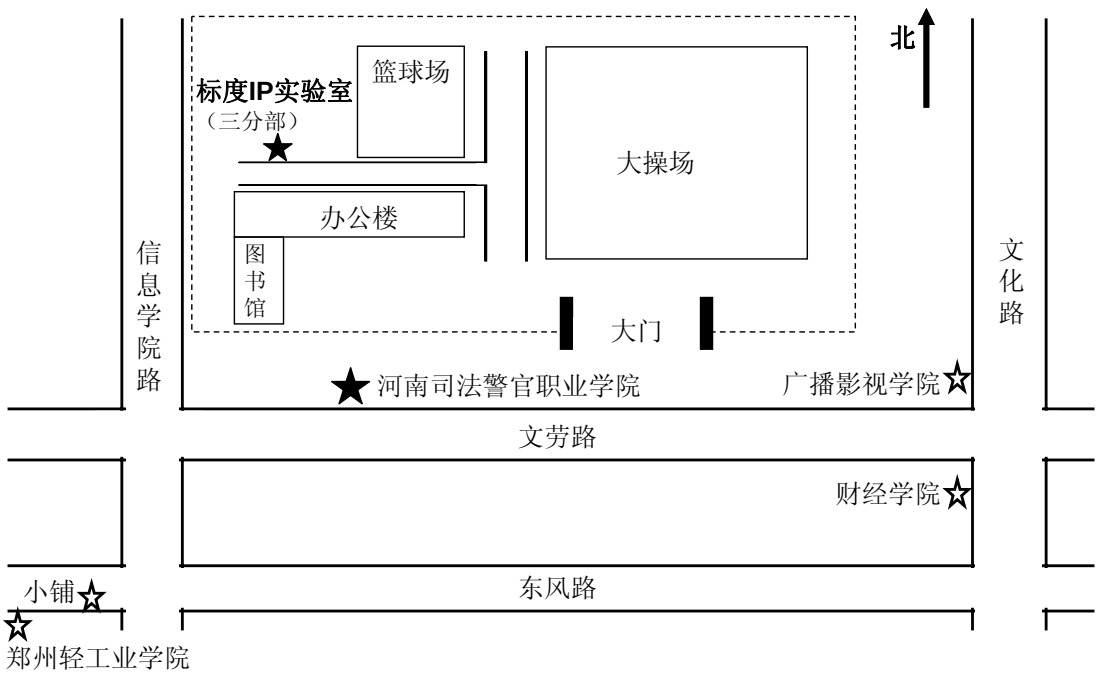
结束语

标度IP实验室将致力于推动河南IT教育产业的发展。我们将以最优秀的师资、最丰富的教学经验及完善的服务，努力推动河南IT行业前进的步伐。

帮助您成为网络工程师、获取高薪工作、创造美好生活是标度IP实验室的一贯宗旨。我们相信，标度IP实验室必将成为您在网络技术领域中发展的良师益友。

河南标度IP实验室

咨询热线：0371—6611 0100；133 2382 3585



乘车路线：

乘6、K6、10、B18、42、83、209、211、332、723、K806路到文化路文劳路站下，大约5分钟路程；

或乘2、28、K28、64、72、86、97、127、506、517、723、K906路到东风路小铺路站下，大约10分钟路程。

乘215到陈寨花卉市场下车，大约10分钟路程