目录

Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南

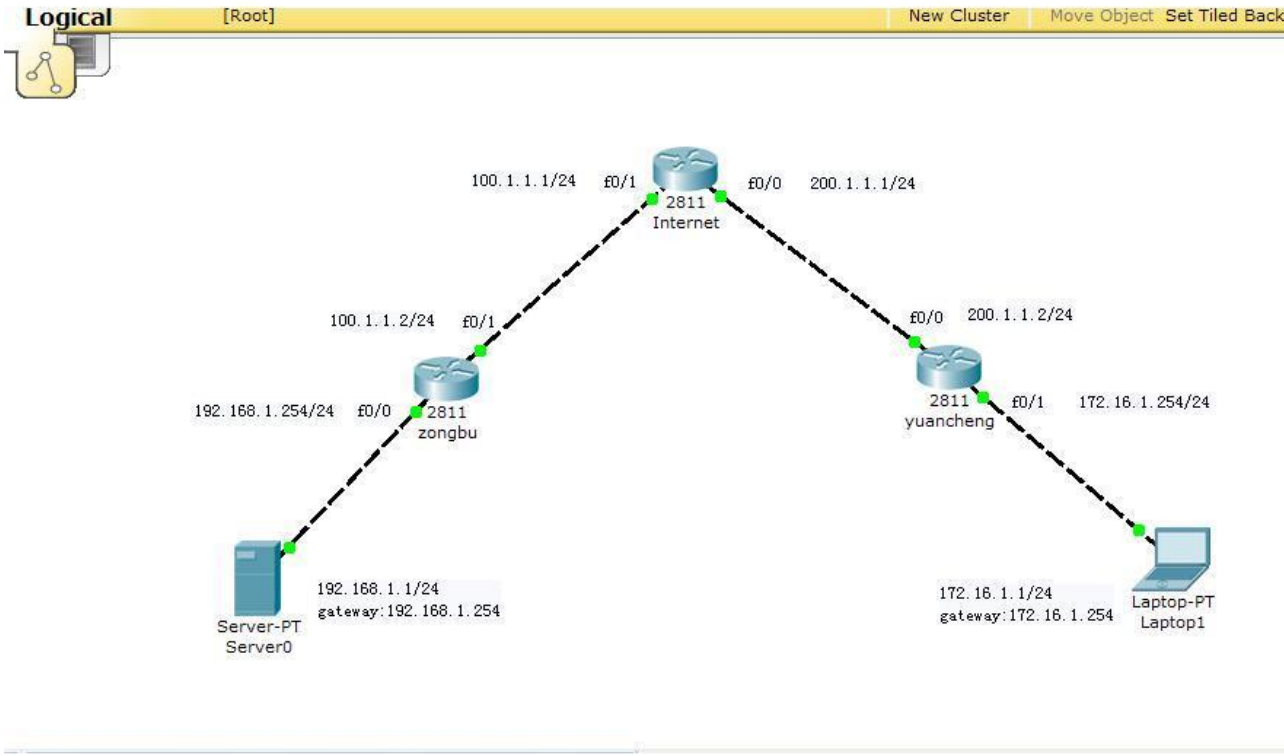
（各位网友注意，从这篇文章开始，我会把已经做好的 Cisco PacketTracer 5.2 的实验 pkt 文件在附件共享，有兴趣的可以下载用 PacketTracer 5.2 实验研究。本篇 Easy VPN 的 pkt 的基本连通性已经做好了，大家按文章的中的 Easy VPN 实验操作，会看到效果的。最后，还请大家有疑问或有更好的想法，请回复留言。因为，技术只有相互交流才有更快更好的进步）

Easy VPN 是 Cisco 独有的远程接入 VPN 技术。Easy VPN 是在 Ipsec VPN 建立的两个阶段（IKE 阶段和 IPSEC 阶段）之间多了一个 2.5 阶段（用户认证阶段等）。远程接入 VPN 的常用作用是为外出办公提供很好接入技术。回想当年的外出的移动办公，那时候还是通过电话线拨号连接到内网访问资源。其网络速之慢，费用之贵，小 T 我就不多说了！现在的外出移动办公接入内网访问资源，常用的是远程 VPN 接入技术，其技术的优点在于网速快、费用低，只要你所在地方能上 Internet 网，那么，你就很享受远程 VPN 接入所带来的好处！（大家有机会用过，就会体会到）。

远程 VPN 接入技术，常见的有 PPTP，L2TP，Easy VPN 以及现在很火的 SSL VPN 等。这些远程 VPN 接入技术优缺点，小 T 我会在以后的给大家聊聊！现在我以 Cisco PacketTracer 5.2 这个模拟器为基础，做 Easy VPN 的实验。（讲得不好，还请大家指点。需要下载这个软件的，见我的博客《PacketTracer 5.2 的 IPsec VPN 实验说明(附 PacketTracer 5.2 下载地址)》）

实验的基本思路是这样的，一台路由器做总部 VPN 网关，一台路由模拟 Internet 网（就是没私有 IP 路由的路由器），一台路由路模拟能上 Internet 网的路由器（也就是做了 NAT 上网）。外出移动办公的笔记本通过能上 Internet 网的路由器 Easy VPN 连接到总部，并访问总部的 web 服务器。

实验拓扑：



IP 地址规划如下：

总部服务器：192.168.1.1、24

总部路由器：fa 0/0 192.168.1.254/24　　fa 0/1 100.1.1.2/24

Internet 网路由器：fa 0/1 100.1.1.2/24　　fa 0/0 200.1.1.1/24

远端路由器：fa 0/0　200.1.1.2/24　　fa 0/1 172.16.1.254/24

办公笔记本：172.16.1.1、24

实验的基本配置如下：

总部路由器：

```
interface FastEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 no shutdown
interface FastEthernet0/1
 ip address 100.1.1.2 255.255.255.0
 no shutdown
ip route 0.0.0.0 0.0.0.0 100.1.1.1
```

Internet 路由器：

```
interface FastEthernet0/0
 ip address 200.1.1.1 255.255.255.0
 no shutdown
interface FastEthernet0/1
 ip address 100.1.1.1 255.255.255.0
no shutdown
```

远端路由器的配置：

```
interface FastEthernet0/0
 ip address 200.1.1.2 255.255.255.0
 ip nat outside
 no shutdown
interface FastEthernet0/1
 ip address 172.16.1.254 255.255.255.0
 ip nat inside
 shutdown
ip nat inside source list 1 interface FastEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 200.1.1.1
access-list 1 permit 172.16.1.0 0.0.0.255
```

此时，远端的笔记本能上网，但不能访问总部内的 Web 服务器。现在在总部做 Easy VPN 的配置。其配置如下：

aaa new-model（开启 AAA 认证）

aaa authentication login eza local （命名 eza，对 eza 认证）

aaa authorization network ezo local（命名 ezo，对 ezo 的事件授权）

username tang password 123（创建用户名密码）

crypto isakmp policy 10（Ipsec 阶段一的安全参数配置）

hash md5

authentication pre-share

group 2

ip local pool ez 192.168.2.1 192.168.2.10(Easy VPN 接入后所分配的地址)

crypto isakmp client configuration group myez（Easy VPN 的组和密码配置）

key 123

pool ez

crypto ipsec transform-set tim esp-3des esp-md5-hmac（IPSec 阶段二的配置）

crypto dynamic-map ezmap 10（动态加密图）

set transform-set tim

reverse-route（反向路由注入）

（以下是对 Easy VPN 的认证，授权配置，list 是调用上面的 AAA 的配置名）

crypto map tom client authentication list eza

crypto map tom isakmp authorization list ezo

crypto map tom client configuration address respond

crypto map tom 10 ipsec-isakmp dynamic ezmap（最后，动态加密图必须有静态绑定）

interface FastEthernet0/1

crypto map tom（绑定到接口）

Easy VPN 的测试：

测试如下：

首先，双击笔记本，打开图，选择 Desktop，再下面选择 command Pormpt，ping 一下总部的公网地址 100.1.1.2，通了后再 ping 内部服务器 192.168.1.1，此时是 ping 不通的，因为我们来没 Easy VPN 接入。

其次，我们依然选择 Desktop 下的 VPN，依次输入如下信息：

GroupName：myez

Group key：123

Host IP(server IP)：100.1.1.2

Username：tang

Password：123

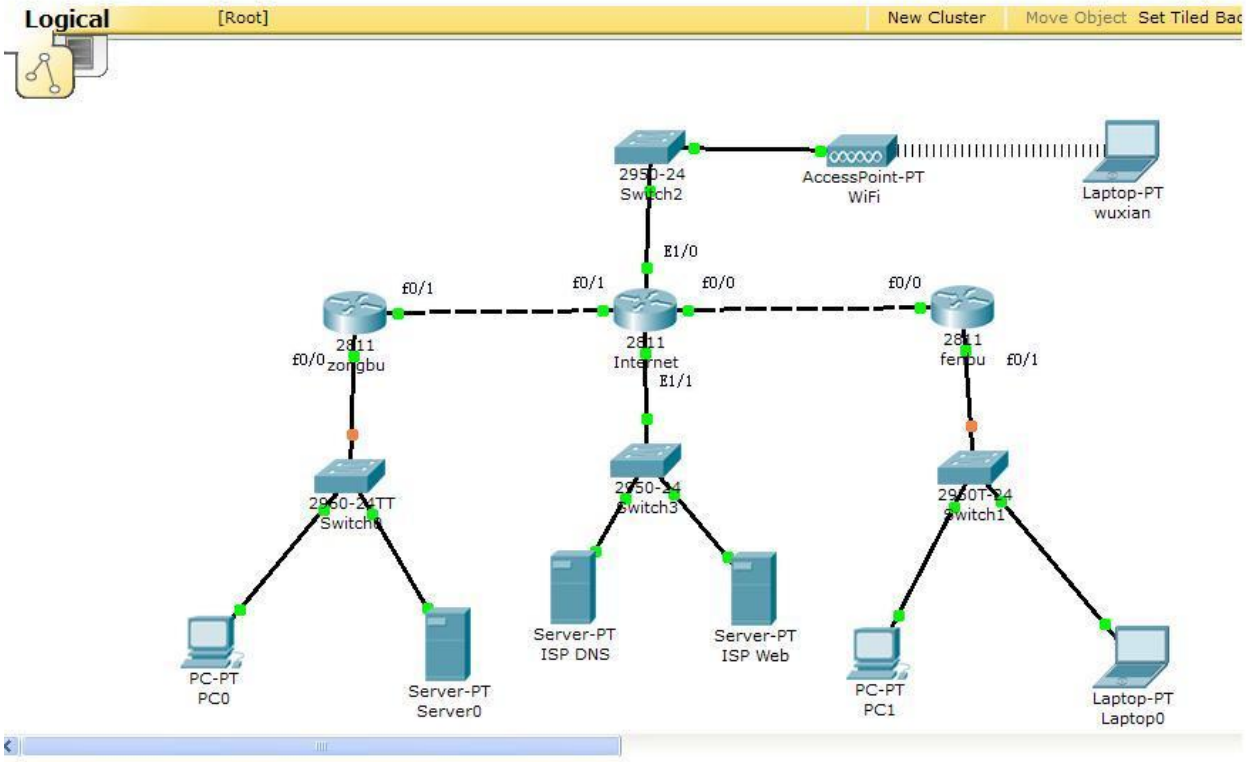
点击 connect，就会提示连接上去，此时会显示下发的 IP 地址。（若没马上连上去，在配置没错的前提下，Ipsec VPN 协商时，前面几个包是不通的，解决方法，在 ping 一下 100.1.1.2，再连接 Easy VPN）。

最后，我们访问 web 服务器，选择 Desktop 下的 Web Browser，输入 IP：192.168.1.1 即可访问到 web 服务器.

PacketTracer5.2 最真实的模拟 VPN 综合实验

本文是由小 T 为大家献上的一道“开胃小菜”，“味道”做的不好，还请大家指点批评。小 T 我努力做到符合大家的“口味”(看不清楚图，请双击放大）！

先简单介绍下本文的模拟真实环境想法！本文是用 Cisco PacketTracer5.2 模拟器（软件下载见我博客的《PacketTracer 5.2 的 IPsec VPN 实验说明(附 PacketTracer 5.2 下载地址)》）做的一个关于 VPN 的综合实验！其基本构想是这样的，最真实的模拟了 ISP 的 DNS 服务器， Web 服务器（简单的讲这个直接挂在 Internet 网的 Web 服务器，就是我们常说的服务器在电信啊，网通啊等 ISP 托管的，日常维护这些服务器都是远程登入上去的！）。用了一个 AP 来模拟移动无线网（你可以想象成我们常用的无线上网，如：GPRS，无线城域网，3G 等。简单点讲就是通过各种无线技术能上 Internet 网）。至于 Internet 网的模拟嘛，还是我常说的没有私有 IP 路由表的路由器。先让大家看看我的实验拓扑：



实验的基本想法，配置思路和测试方法如下：（在附件中有本实验的 PKT 文件下载，大家可以按本文实验。至于 IPSEC VPN 讲解和远程的 Easy VPN 我就不讲解了！大家见我的博客《PacketTracer 5.2 的 IPsec VPN 实验说明(附 PacketTracer 5.2 下载地址)》和《Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南》）。

实验的 IP 规划如下：

PC0 PC1 :DHCP 获取

笔记本：laptop0 和 wuxian：DHCP 获取

内部服务器：Web 192.168.1.253/24 TFTP 192.168.1.252/24

ISP 服务器：ISP DNS 202.103.96.112/24 ISP Web 202.103.96.120/24

总部 fa0/0:192.168.1.254/24 fa0/1:100.1.1.2/24

Internet 网：fa0/1 :100.1.1.1/24　　fa 0/0:200.1.1.1/24

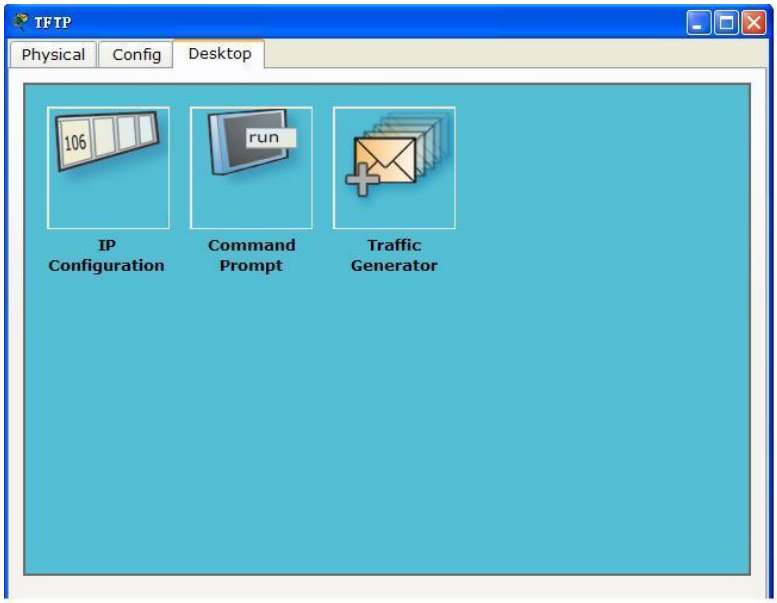
E1/0:210.1.1.1/24(移动笔记本 wuxian 所获得公网地址段)

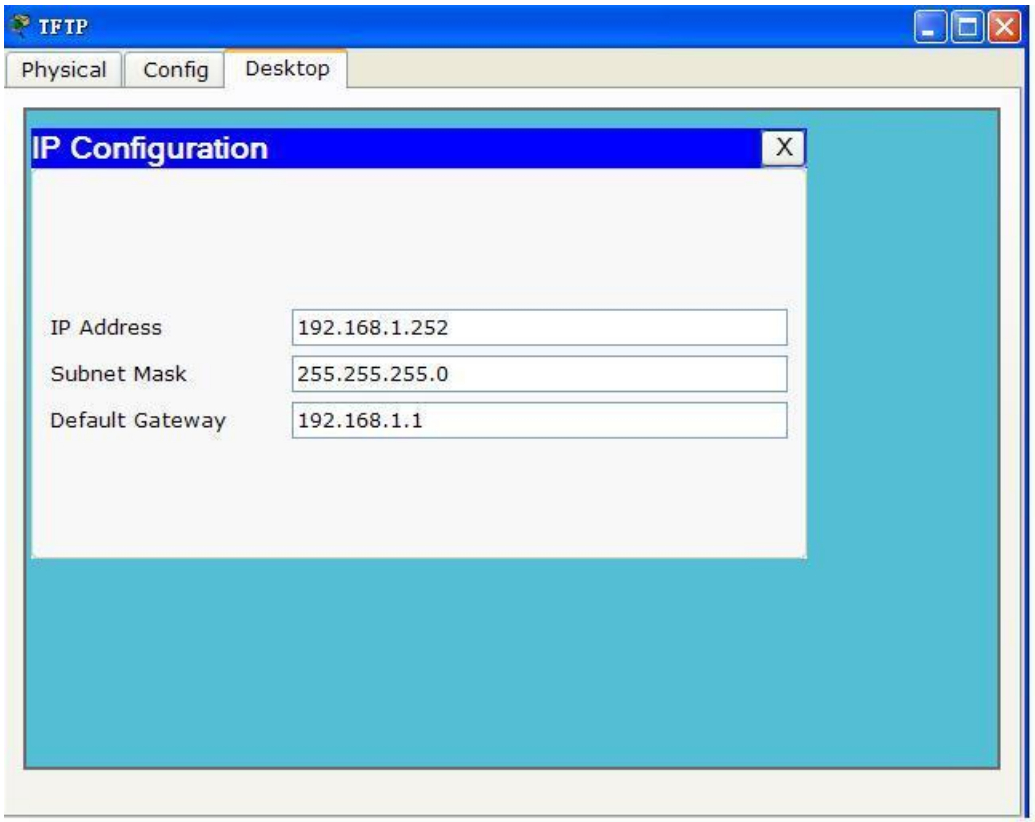
E1/1:202.103.96.1/24(ISP DNS 和 ISP Web 服务器的网关)

分部：f0/0:200.1.1.2/24　fa 0/1:192.168.2.254/24

关于 PacketTracer5.2 中的服务器 DNS 和 Web 的配置以及 PC 和笔记本的配置和测试。如图说明：

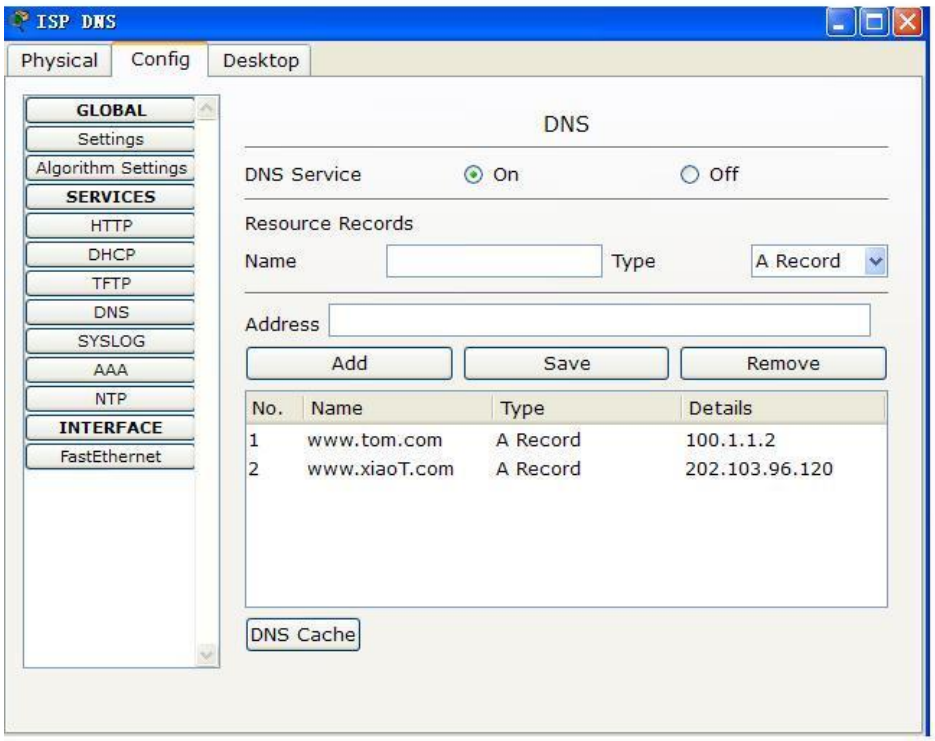
双击服务器的图标，选择 Desktop，在选择 IP configuration 设置 IP 地址：





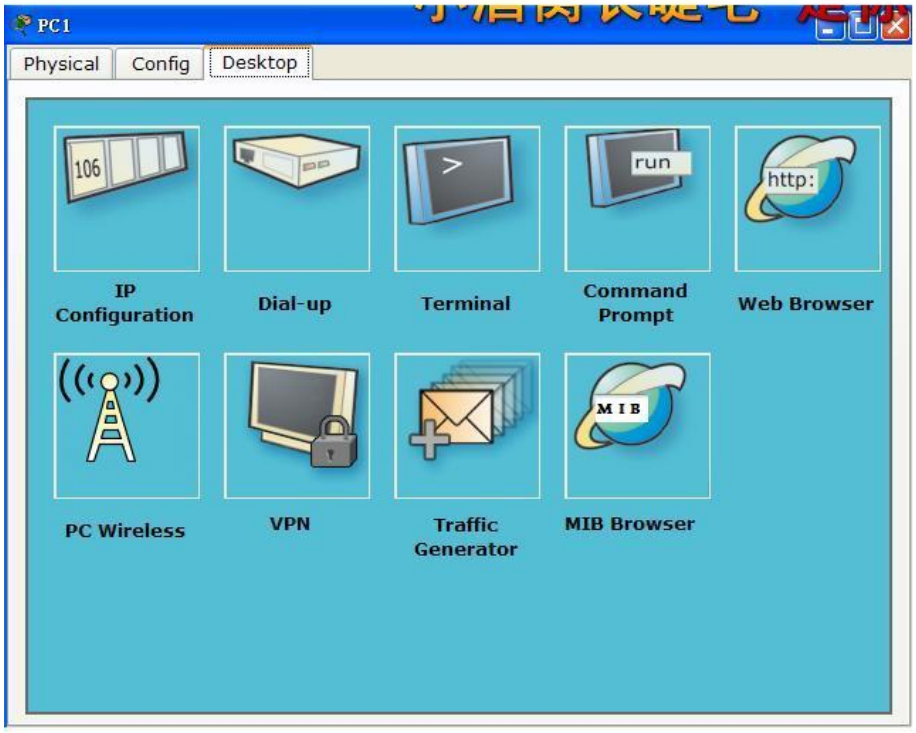
DNS 的配置：（我为 ISP 的 Web 服务器和总部的 Web 服务器做的 DNS 映射）

选择如图一的 config，在选择 DNS，name 是域名，address 是 IP 地址，做好就 add 添加。



Web 服务器的配置，就点 HTTP，自己可以修改 Html。这我就不讲了，记得服务 On。

PC 和笔记的配置结构一样如图：



本次试验用到了，IP configuration、Web Brower，VPN，command Prompt。

IP configuration 是 IP 的配置：可以 DHCP 也可静态。

Web Brower 是浏览器。VPN 是 Easy VPN 客户端。

command Prompt 就是 CMD，用 Ping 的测试等。

实验基本连通性：

Internet 网配置：

enable

configure terminal

```
hostname Internet
line console 0
logg sy
exec-time 0 0
exit
no ip domain-lookup
interface fastethernet 0/1
ip add 100.1.1.1 255.255.255.0
no shut
exit
interface fastethernet 0/0
ip add 200.1.1.1 255.255.255.0
no shut
exit
interface ethernet 1/1
ip add 202.103.96.1 255.255.255.0
no shut
exit
interface ethernet 1/0
ip add 210.1.1.1 255.255.255.0
no shut
exit
ip dhcp excluded-address 210.1.1.1
ip dhcp pool wifi
 network 210.1.1.0 255.255.255.0
 default-router 210.1.1.1
 dns-server 202.103.96.112
 exit
```

总部配置：

```
enable
configure terminal
hostname Internet
line console 0
logg sy
exec-time 0 0
exit
no ip domain-lookup
interface fastethernet 0/1
ip add 100.1.1.2 255.255.255.0
no shut
ip nat outside
exit
interface fastethernet 0/0
ip add 192.168.1.254 255.255.255.0
no shut
ip nat inside
exit
ip route 0.0.0.0 0.0.0.0 100.1.1.1
ip dhcp excluded-address 192.168.1.254
ip dhcp pool zongbu
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.254
 dns-server 202.103.96.112
 exit
access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.2
55
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
```

```
ip nat inside source list 100 interface FastEthernet0/1 overload
ip nat inside source static tcp 192.168.1.253 80 100.1.1.2 80
```

分部配置：

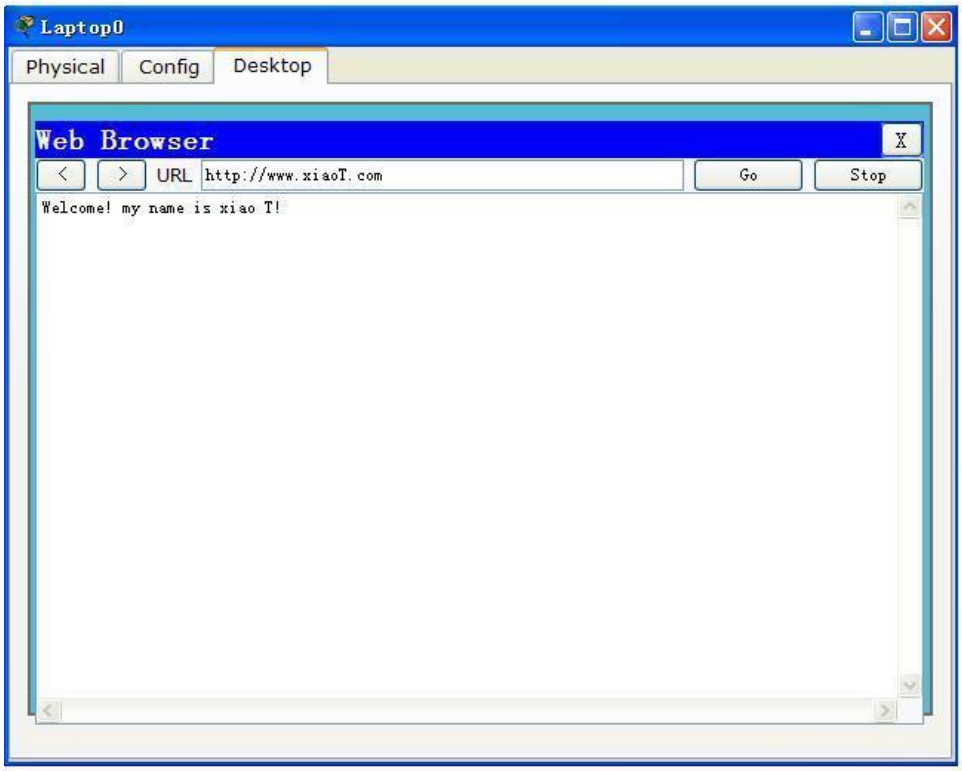
```
enable
configure terminal
hostname fenbu
line console 0
logg sy
exec-time 0 0
exit
no ip domain-lookup
interface fastethernet 0/0
ip add 200.1.1.2 255.255.255.0
no shut
ip nat outside
exit
interface fastethernet 0/1
ip add 192.168.2.254 255.255.255.0
no shut
ip nat inside
exit
ip route 0.0.0.0 0.0.0.0 200.1.1.1
ip dhcp excluded-address 192.168.2.254
ip dhcp pool zongbu
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.254
 dns-server 202.103.96.112
 exit
```

access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 192.168.2.0 0.0.0.255 any

ip nat inside source list 100 interface FastEthernet0/0 overload

当基本连通性结果后，在浏览器中访问：www.xiaoT.com 和 www.tom.com 结果如下图：



但由于 VPN 没有做，外网和分部的 PC 是 Ping 不通内部的 PC 和服务器的。

现在进行 VPN 配置：

总部：

```
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share

crypto isakmp key tom address 200.1.1.2

crypto ipsec transform-set tim esp-3des esp-md5-hmac

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.
255



crypto map tom 11 ipsec-isakmp
set peer 200.1.1.2
set transform-set tim
match address 101

interface FastEthernet0/1
crypto map tom

aaa new-model
aaa authentication login eza local
aaa authorization network ezo local
username tang password 123

ip local pool ez 192.168.3.1 192.168.3.100
crypto isakmp client configuration group myez
```

```
 key 123
 pool ez

crypto dynamic-map ezmap 10
 set transform-set tim
 reverse-route

crypto map tom client authentication list eza
crypto map tom isakmp authorization list ezo
crypto map tom client configuration address respond
crypto map tom 10 ipsec-isakmp dynamic ezmap
```

（Easy VPN 是 IPSEC VPN 的两个阶段之间的 2.5 阶段，固阶段一喝阶段二都可以条用一样的策略）

分部的配置：

```
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share

crypto isakmp key tom address 100.1.1.2

crypto ipsec transform-set tim esp-3des esp-md5-hmac

crypto map tom 10 ipsec-isakmp
set peer 100.1.1.2
set transform-set tim
match address 101
```

access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

interface FastEthernet0/0

crypto map tom

测试：

Ipsec VPN 就是分部的 ping 总部的 PC，来检测连通性，Easy VPN 的连接测试在《Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南》中有说明。

当 VPN 都连通后，就能 ping 通内部的 TFTP 服务器了！

最后给大家留个问题，本实验中，我已经解决了，Ipsec VPN 的 VPN 和 NAT 上网问题。但我无线笔记 Easy VPN 接入总部后，只能访问用 IP 来访问内部 Web 服务器，而访问不了 Internet 的 Web 服务器。这是为什么，应该如何解决。

（附件中，有基本连通的 PKT 文件，和最终完成 PKT，有兴趣的网友可以按我的配置做实验。）http://9916376.blog.51cto.com/468239/197253

浅谈 PacketTracer 5.2 模拟器

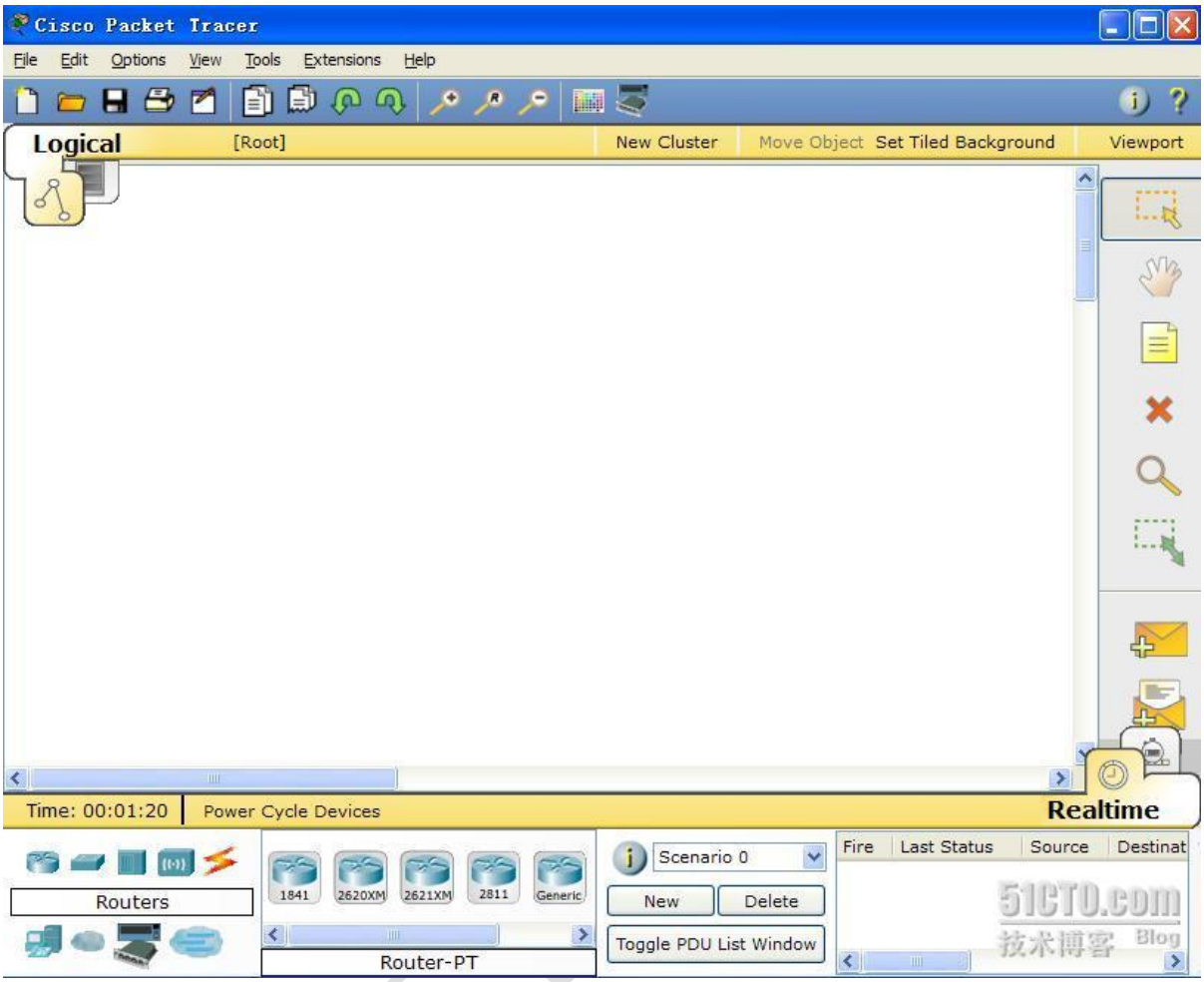
前言 在我的博客一文《【分享】我与网络技术的那些故事》中讲述了，我学习 cisco 技术是从玩各种模拟器开始的。像最简单的一点通模拟器，我也下载过来玩过。呵呵。。。在我所玩过的模拟器中，个人觉得 PacketTracer 系列的模拟器，对初学网络技术存在很多的好处的。本文献给那些 cisco 网络初学者以及 PacketTracer 模拟器的爱好者。

说到玩这款模拟器，小 T 我也只玩会了 30%左右，所以在各位面前不敢以专家自居。在我所玩过的模拟器中，PacketTracer 系列模拟器给与人最真实的网络拓扑视觉感和网络效果感觉，，我相信大家在学习 cisco 网络技术的时候，最想看到的时候整个网络调试好后的效果吧！PacketTracer 系列模拟器还有一个最大的优点在于能让初学者在学习数据包结构、协议包结构有好的入门帮助效果，但 PacketTracer 系列模拟器最吸引我的地方，则是它的数据流演示效果，这对形成良好的数据流意识很有帮助（我在我博客一文《【分享】我与网络技术的那些故事》中已经阐明了数据流意识在学习和分析网络问题的重要意义）。

现在，让小 T 我给讲浅谈一下 PacketTracer 的基本操作和它是如何体现我所说的好处。

首先，我们了解了解下 PacketTracer 的各个作用和基本操作。

如图所示，展示着 PacketTracer 5.2 大体。



现在由我小 T 慢慢跟大家大概聊聊这款模拟器的界面。中间的那个很大的空白区域就是让我们画网络拓扑滴。左下角(如下图)的区域是网络设备区域：

在上图中，左边是网络设备的各种类型，先做简单的说明，从右边开始，第一个圆形是路由器，当你把点击路由器，会在右边显示各类路由器的型号，这些路由器都集成多业务路由器。紧接着是交换机，同样你点击交换机，也会看到各种型号（后面就不重复说各个型号了，大家自己看看吧。）再过来过来的是集线

器（HUB）。在集线器的右边那个就是无线设备，里面有 AP 和无线路由器。红色闪电形状就是各类线缆，等下稍作重点给大家讲讲！下面的 PC 图标中，包括了个人 PC，笔记本，服务器，打印机还有 IP 电话（哎。。。打印机和 IP 电话是配角，好看的）。云的的形状是模拟了广域网，如帧中继、等（具体的大家慢慢看吧！）。至于之后两个图标，小 T 我一直没弄明白有什么意义，期待高手给我解答。

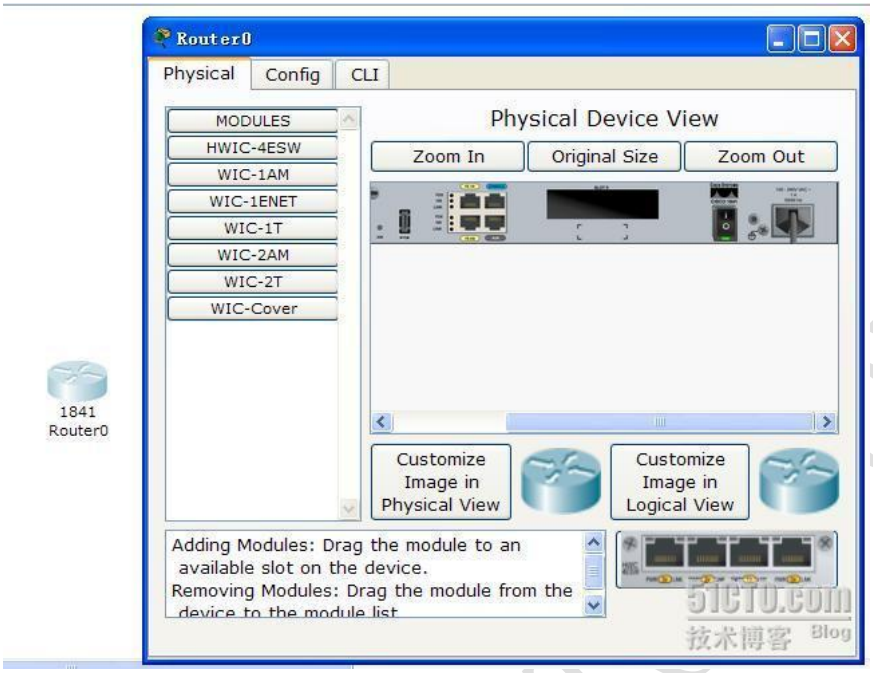
现在给大家讲讲线缆的图标，如果实验的时候，接错线缆的，那做实验就会很压抑了。双击红色闪电图标，展示如下图：

第一个闪电符号，那是自动连线，对线缆不熟的初学者可以用这个来连接网络设备。第二根就是我们常用的 console 线，只要是在连接电脑的 R232 和网络 console 口，在新的网络设备，一般都要靠这跟线来调试。嘿嘿的直线就是我们常用说的直通线，两头都是 568B 或者 568A 的线序。虚线的直线就是我们交叉线，不要是用来连接相同设备的，不过，现在的网络厂商都做到了自适应识别。交叉线旁边就是我们所说的光纤了，只有路由器或者交互机上有光纤接口，就用此线连接。虚线的闪电符号就是电话线（小 T 我一直没做过电话的的实验，也不知道从哪下手，期待高手指点）。电话线旁的就是铜轴电缆了（没怎么用过）。最后的两个红色闪电号，带时钟的是接 DCE 设备的串口线，没时钟是接 DTE 设备的串口线（说实话，我们现实网络实施中，DCE 设备电信等 ISP 的设备，我们只要确保我们的设备没问题，剩下的问题交给电信的去处理，在试验的时候需要一个路由器做 DCE，也就是配置了时钟频率的 serial 接口）！

至于右边的那些菜单键，大家慢慢玩，很快就明白了。最下面的两个信封是用测试网络连通性的。

再来说说，这款模拟器在给人的真实的一点感觉吧！（以路由器为例，其他的都差不多）。

在这款模拟器中，路由器都是集成多业务路由器，可以更换网络模块的！下面是路由器的图：



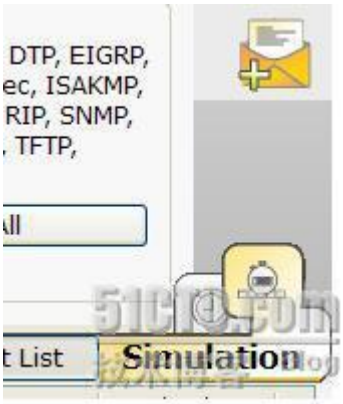
双击路由器就会看到，右边的图，大家注意 Physical 是物理特性，最左边的是网络接口卡，若想换网网络接口在右边的图中，先关掉电源，在把左下角的网络接口拖到相应大小的模块中。点击中间的 config，你可以理解为 Web 图形配置。CLI 还是大家熟悉的命令行，我就不多说了。

网络实验中，最常用来测试的 PC 是少不了的。下图，便是 PC 在这款模拟器中，常用到的工具。

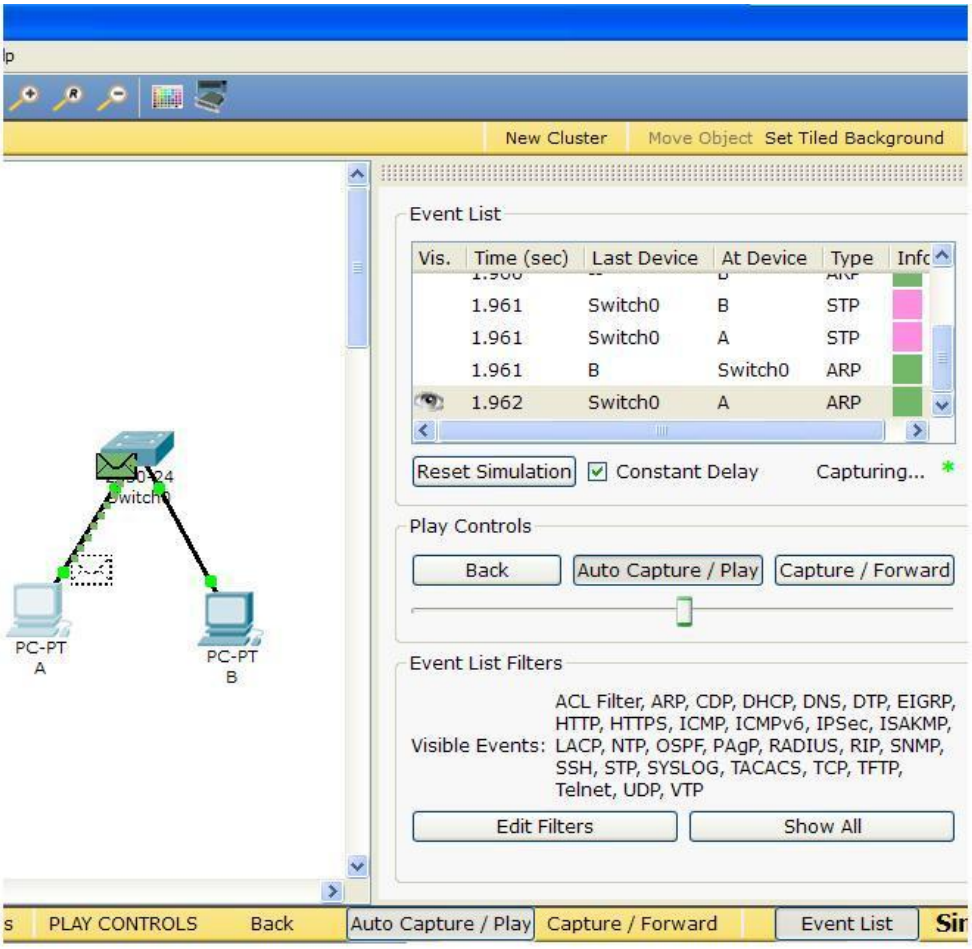
双击 PC 就会看到上图的内容。Physical 跟路由器一样，可以换网卡。Config 也是一样。Desktop 这里面得东西，在测试的时候给人感觉是最真实的。IP configuration 是 IP 地址配置；isl-up 这个小 T 我只能猜测是电话线拨号上网的，待高手指点这个的功能；erminal 就是超级终端，在现实中新的网络设备一般都要通过它来调试；command prompt 就是 CMD，可以用来 telnet、ping、trace 等；web Brower 是网页浏览器；PC Wireless 网卡换成无线的时候，与无线 AP 和无线路由器时，就可以调试；VPN 是 Easvy VPN 客户端;Traffic General 是数据和协议测试工具（小 T 我没玩过，这是 5.2 增加的功能）；最后是应该是做 SMNP 实验的（也是 5.2 新增加的功能，小 T 还不会 SMNP 的实验，还期待高手指点）。

在前面我一直强调这款模拟器的数据流效果，现在我就来给大家简单的介绍下！

首先，从实训模拟切换“流分析模式”（这是我小 T 对他的称呼），如如操作。

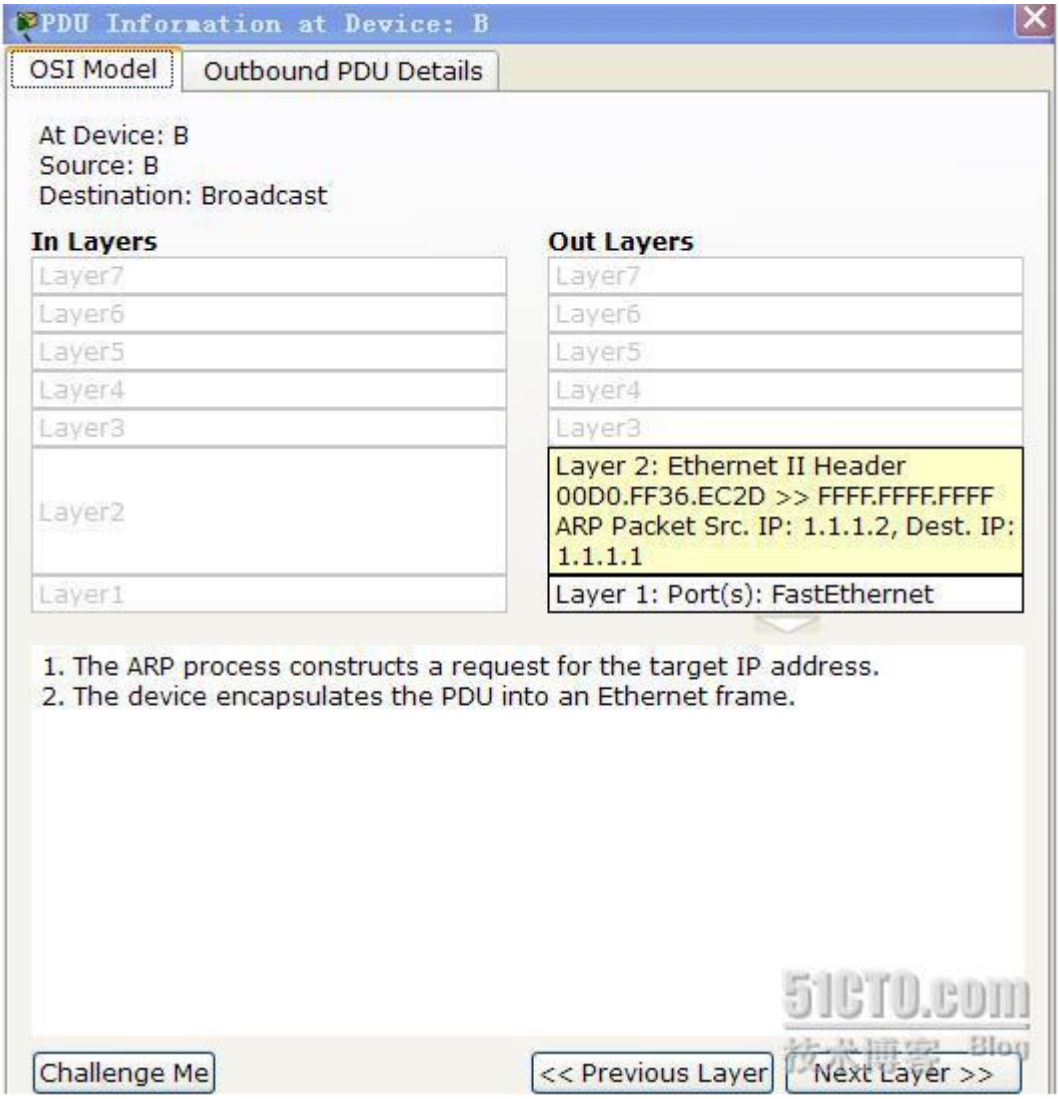


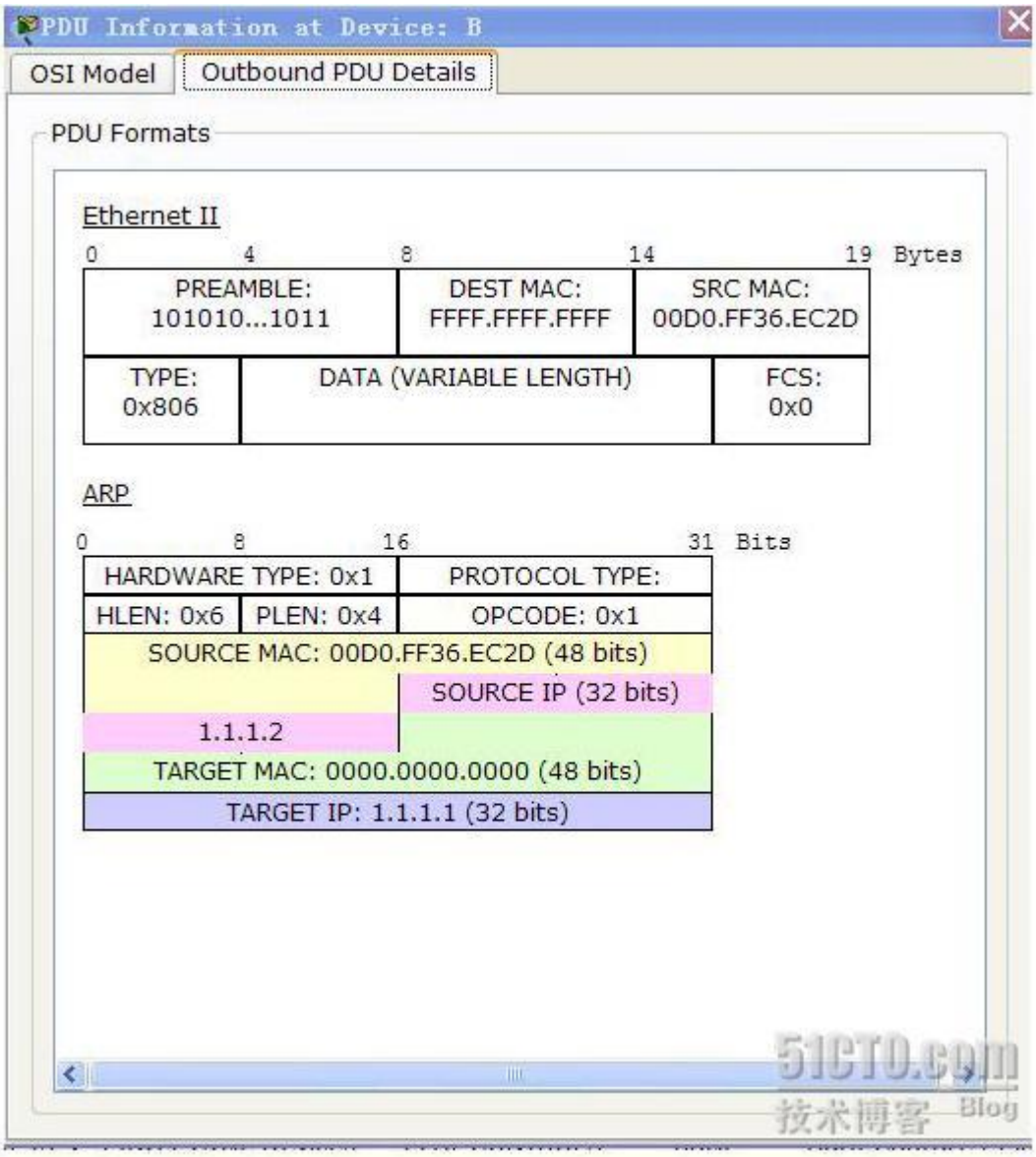
只要点击中下 Realtime 后面的，就会切换到我所说的“流分析模式”，（我的网络拓扑图，就是以我博客一文中的《【分享】我与网络技术的那些故事》中的数据流分析为例的，如果，大家想看数据流分析，请到这篇文章看看。）效果如图：



呵呵。。。图中绿色的信封正在流动，代表着 ARP 数据流向。怎样操作才能看到数据流呢！很简单，首先大家点击图中的 Auto capture/play,再在最右边的工具栏中，选择信封带＋号的，现在主机 A 上点一下，再到主机 B 上点一下，数据流效果就出来了。还有很多功能在这图中，大家慢慢摸索吧！

形成数据流意识很重要，要理解数据流就必须理解包和协议包的数据结构，要了解这些，就必须掌握好 TCP/IP 原理。若你想在这款模拟器中，看到数据结构，只要先让 Auto capture/play 停止，选择左上图的数据包，在左边的拓扑中，就会有哪种相应颜色的数据包停留在上面，只要双击就可以看到效果。下面两张就是效果图：


PDU Information at Device: B
OSI Model
Outbound PDU Details
At Device: B
Source: B
Destination: Broadcast
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1
Layer 2: Ethernet II Header
00D0.FF36.EC2D >> FFFF.FFFF.FFFF
ARP Packet Src. IP: 1.1.1.2, Dest. IP: 1.1.1.1
Layer 1: Port(s): FastEthernet
1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.
Challenge Me
<< Previous Layer
Next Layer >>



最后，我还是那句话，技术只有多交流才有更好更快的进步！

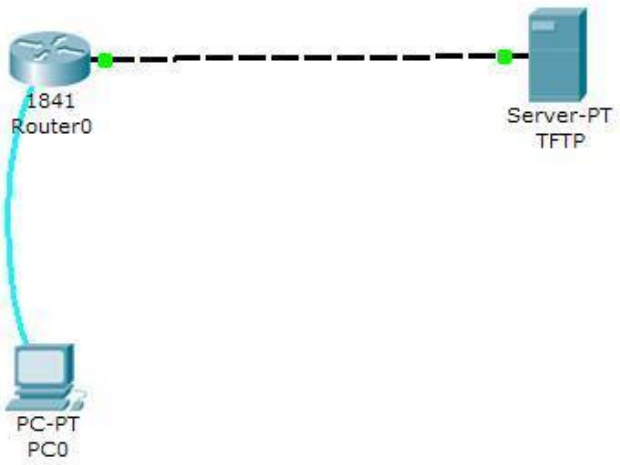
PacketTracer 5.2 之路由器 IOS 升级实验指南

（从这篇文章开始，小 T 我开始从简单的实验开始写起，希望对网络学习者有所帮助。用于模拟功能有限，小 T 只好写写路由器从 TFTP 升级 IOS 的了。）

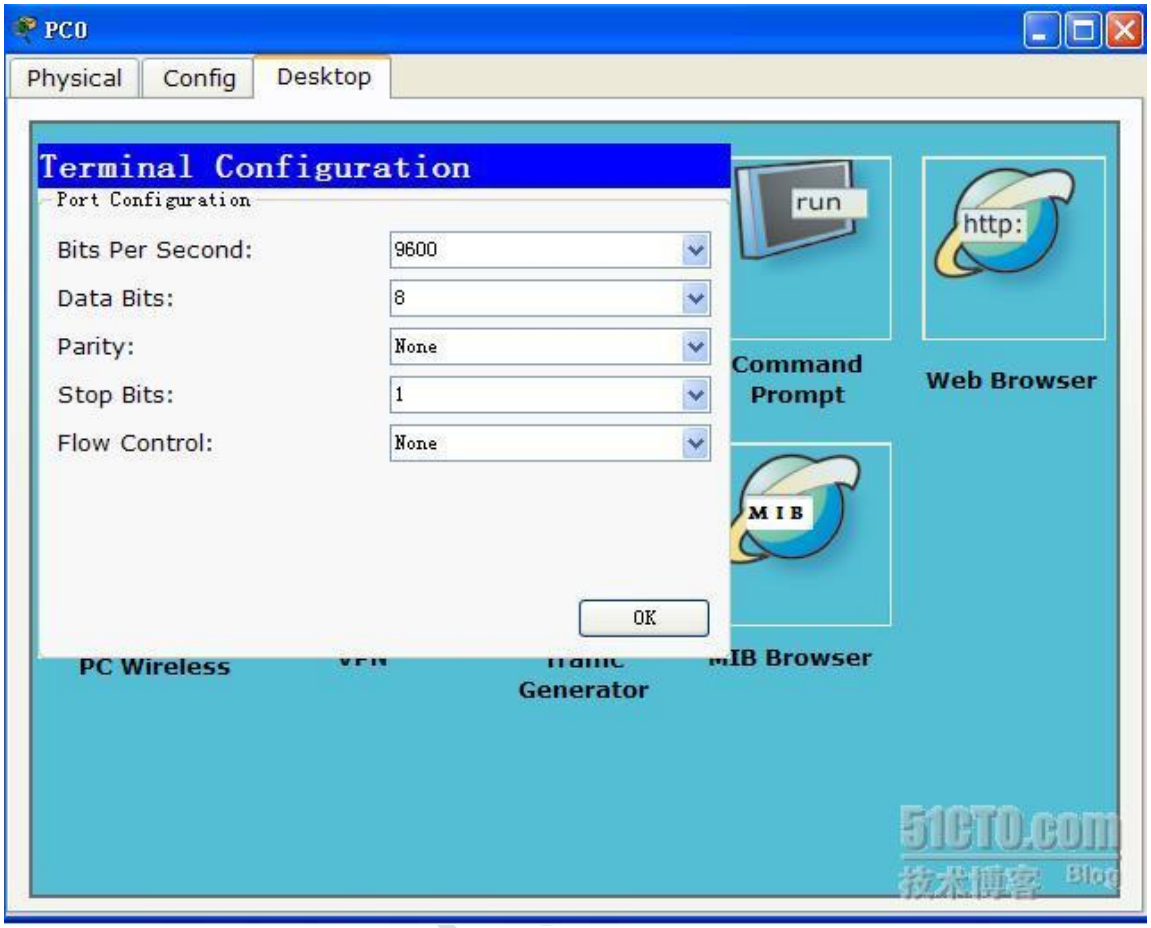
路由器实际上就是一种特俗用途的计算机，和常见的 PC 一样，路由器有 CPU，内存和 BOOT ROM 但路由器没有键盘、硬盘和显示器；然而比起计算机，路由器多了 NVRAM、FLASH 及各种各样的接口。IOS 其实就是 cisco 路由器、交换机等网络设备操作系统，这是一种嵌入式系统（像国内的一的一些厂商，其实就 Linux 嵌入式开发的系统）。IOS 的版本决定的路由器能完成什么样的功能，就想我们的 Windows 操作系统一样，Windows server 版本就能做服务器，xp 还能充当客户机角色了。IOS 的版本也是这样的，举个例子吧：c1841-ipbase-mz.123-14.T7.bin 这个就是一个最基本的基本的版本，如果你拿它去做 Ipsec VPN，不好意思，这个 IOS 不支持。C1841-advipsevicek9-mz.124-15.T1.bin 这个版本就能支持 Ipsec VPN。故升级 IOS 是更加充分发挥路由器的功能。

简单讲讲常见的 IOS 升级吧，方法有从 console 口导入，从 TFTP 服务器上导入，从 TFP 服务器上导入等等。相比而言，现在大多数人喜欢用 TFTP 升级（TFTP 软件网上很多，下载到自己电脑上，你的电脑就成了 TFTP 服务器），因为，console 升级太慢了，一个 10M 的 IOS 升级要 3 到 4 个小时；FTP 繁琐点，要用户名啊，密码等；TFTP 就简单多了，从 100M/S 的网线升级 IOS，只要几分中就行了！

现在就讲讲 IOS 的升级实验，拓扑见下图：

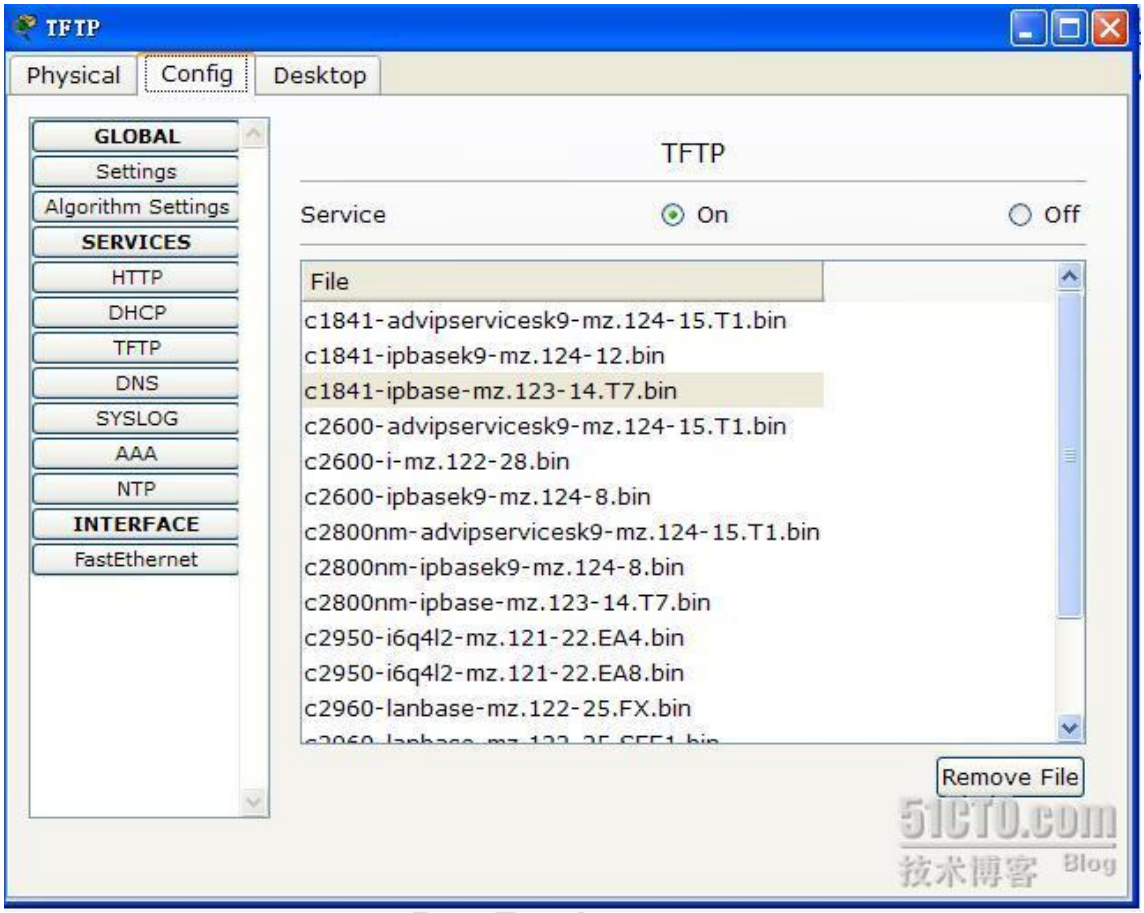


主要是 PacketTracer 5.2 的 PC 没有 TFTP 功能，现实中，网线和 console 都是接再我们的电脑上的！简单 IP 说明：路由器 fa 0/0 10.1.1.1；TFTP 服务器 10.1.1.2。我从 PC 中的超级终端登入到路由器上面，选则 PC 的 Desk Top 中 Terminal（如图配置）



点击 OK 进入。现实中，我们 Windows 的超级终端打开：开始——>所有程序——>附件——>通讯——>超级终端。点击还原默认值就跟上图的信息一样了。

在 PacketTracer 5.2 中的 TFTP 服务器中有（如图）各种型号的 IOS，大家根据路由器的型号升级 IOS。



先 show version 命令看看当前我们的版本：

R1#show version

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on

System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

（这已经是高级版本了，为演示实验，我把它升级到底的版本）

先 ping 一下服务器的 IP 地址是否连通，连通后就可以从 TFTP 升级 IOS 了。升级 IOS 命令如下：

R1#copy tftp: flash: （从 TFTP 服务器上将 IOS 拷贝到本地 FLASH 中）

Address or name of remote host []? 10.1.1.2(TFTP 服务器的 IP 地址)

Source filename []? c1841-ipbase-mz.123-14.T7.bin（TFTP 服务器上的原文件名）

Destination filename [c1841-ipbase-mz.123-14.T7.bin]? (copy 到路由器 FLASH 上的文件名)

Accessing tftp://10.1.1.2/c1841-ipbase-mz.123-14.T7.bin...

Loading c1841-ipbase-mz.123-14.T7.bin from 10.1.1.2:

!!!

!!!

!!!

!!!

[OK - 13832032 bytes]

（注意：在 Flash 空间做够大的情况足够大的情况下，IOS 是导入没问题的，我的演示上面是空间够得；空间不足的时候，则选择覆盖原来的 IOS，这是你在 flash 中看的名字还是原来名字，但你 show version 看版本就能看到已经升级成功得版本了）

在空间足够大情况下，你就会看到 Flash 中有两个操作系统。

R1#show flash:

System flash directory:

File	Length	Name/status
3	33591768	c1841-advipservicesk9-mz.124-15.T1.bin
4	13832032	c1841-ipbase-mz.123-14.T7.bin
2	28282	sigdef-category.xml
1	227537	sigdef-default.xml

[47679619 bytes used, 16336765 available, 64016384 total]

63488K bytes of processor board System flash (Read/Write)

这时候我们只要在全局模式下敲如下命令，来引导 IOS。

R1(config)#boot system flash c1841-ipbase-mz.123-14.T7.bin

然后重启路由器，你 show version 就可看你到升级后的版本。

路由器也可以做ＴＦＴＰ服务器，只要输入如下命令，你的路由器就能从另一台路由器上升级 IOS，但模拟器不支持。

R1(config) tftp-server flash c1841-ipbase-mz.123-14.T7.bin

如果你一不小心把 IOS 的删掉了，在以前老的 cisco 路由器上，那你就慢慢等等 4 个小时从 console 升级吧。不过现在的 cisco 的多业务集成路由器，就能在 ROM 模式下升级 IOS，这可解救了我们啊！操作命令如下：

rommon 1 > IP_ADDRESS=10.1.1.1

rommon 2 > IP_SUBNET_MASK=255.255.0.0

rommon 3 > DEFAULT_GATEWAY=10.1.1.2

rommon 4 > TFTP_SERVER=10.1.1.2

rommon 5 > TFTP_FILE=c1841-ipbase-mz.123-14.T7.bin

rommon 6 > tftpdnld

会提示你是否配置正确，你选择“Y”，升级完后 boot 启动就可以了。

PacketTracer 5.2 之交换机和路由器的维护实验

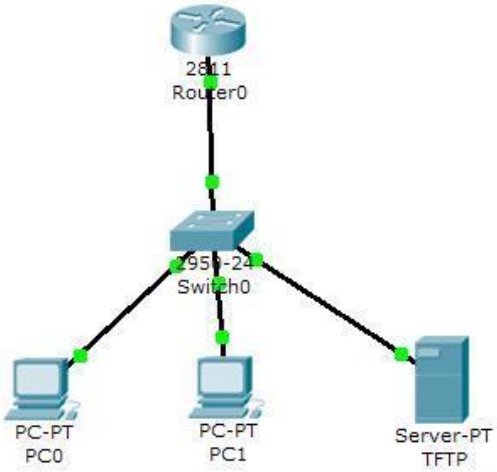
（注：图片看不清，请点击放大）

每当一个网络项目完成后，日后的日常网络维护就交给了网络管理员来维护。一般对网络设备的维护，小 T 我大概总结为，备份和还原网络设备的操作系统，备份和还原设备的配置文件，网络设备密码遗忘了如何恢复，对 telnet、SSH、Web 等管理设置密码及身份认证，根据新增的需求配置网络设备等。

作为一名网络维护人员，在新接手一台已经调试好网络设备的时候，首先要做的事情，就是将网络的设备的配置文件保存。这样的做的好处，是为以后设备出问题了，还有一招最后的解救方法。所以，备份网络设备的配置文件，对每位网络维护人员来说是很重要的。若网络设备的操作系统（cisco 的是 IOS，H3C 是 VRP）可以导出来的话，我们就将网络设备操作系统备份。备份网络操作系统，这是为了防止哪天网络操作不小心操作失误，把网络设备操作系统给弄“坏”了，好有地方找到网络操作系统给它还原。谁都会有忘记一些东西的时候，作为网络维护人员，忘记网络设备的密码的情况也是避免不了的，但必须学会密码恢复。所以，小 T 我个人对每位网络维护人员的建议就是，要了解你们所掌管的网络设备如何做密码恢复的。如果我上面说的这几点，你没做到话！网络设备出问题了，那就打卖设备给的你公司，叫他们给你维护，每次多花点钱而已。

在开始今天的实验之前，小 T 先讲讲实验思路。在这次试验中，我还是采用通过 TFTP 的备份方法，当然你也可以用 TFP 等。首先，讲讲 cisco 设备的配置文件，常看到的是：startup-config 和 running-config。Runing-config 是 cisco 设备的当前运行文件，断电是不保存的，我们配置完了 cisco 设备，都是在的文件中。startup-config 是 cisco 的启动配置文件，也就是说，cisco 的设备在启动经历了加电自检，加载 IOS，再加载 startup-config 文件。所以，我们在配置完 cisco 的设备的时候，记住敲上 copy running-config startup-config 或 write 在保存配置文件，不然，你重启后，你的网络设备啥东西也没有了！当我们遗忘了密码，通过了解网络设备启动过程，我们只要想办法让设备不加载 startup-config 文件，就有办法恢复密码。（cisco 的路由器是通过路由器修改寄存值；而交换机则是采取将这个文件名修改一下，由于模拟器不支持，故小 T 我只给大家描述下）。

先让大家看看我的实验拓扑：



通过模拟一个小小的局域网，便于让大家来理解。PC0、PC1、TFTP 服务器不在同一个网段，解决相互通信采用了单臂路由。

IP 的规划如下：

PC0：192.168.2.1/24

PC1:192.168.3.1/24

TFTP:192.168.1.2/24

交换机管理 IP：192.168.1.1/24

实验的基本连通性配置：

路由器的配置：

```
enable
config t
line console 0
logg sy
exec-time 0 0
exit
hostname R1
```

```
interface FastEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 no shut
interface FastEthernet0/0.1
 encapsulation dot1Q 2
 ip address 192.168.2.254 255.255.255.0
 no shut
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.254 255.255.255.0
 no shut
```

交换机的配置：

```
enable
conf t
line console 0
logg sy
exec-time 0 0
exit
vlan 2 name vlan2
vlan 3 name vlan3
interface range fastEthernet 0/1 -5
switchport mode access
switchport access vlan 2
spanning-tree portfast
exit
interface range fastEthernet 0/6 -10
switchport mode access
switchport access vlan 3
```

```
spanning-tree portfast
exit
interface fastEthernet 0/24
switchport mode turnk
exit
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
 no shut
exit
ip default-gateway 192.168.1.254（不同网段要想能 ping 和访问必须为交换机配置网关）
```

所有网络设备和 PC、服务器的联通性解决了，那么我们先从登入的密码身份认证开始试验。

登入 cisco 网络设备，常用的是通过 console 口直接连接，远程 telnet，安全的远程 SSH，以及 web 访问。由于模拟器不支持 Web，故本实验演示前面三种。

一、密码访问登入

Console：

```
line console 0
password xiaot
login
```

当你配置上这些命令的时候，你 console 口登入就会如下提示输入密码。

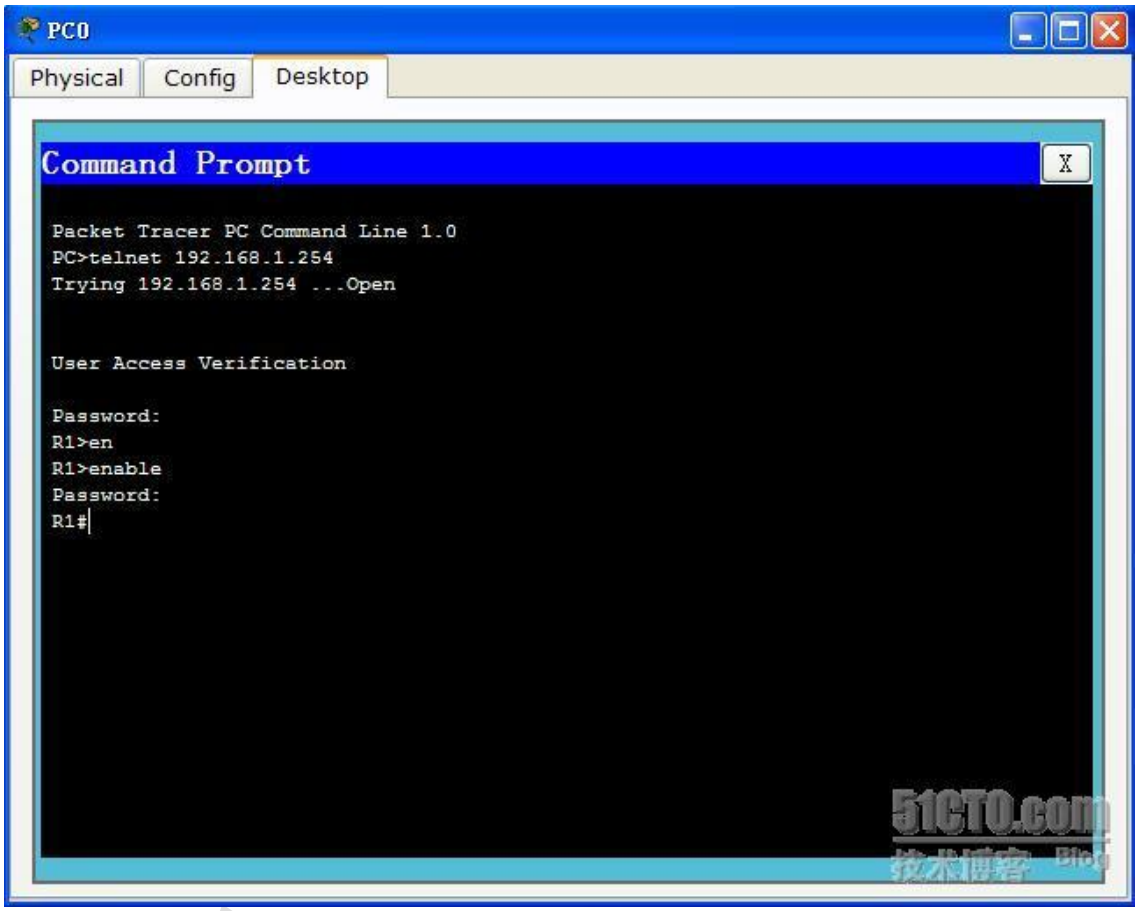
```
Password:
R1>
```

telnet：

```
line vty 0 4（这表示从 0-4，有五个用户可以同时登入）
password xiaot
login
```

enable password 123（此密码必须配置，不然你就只能停留在用户模式）

测试在 PC 的 CMD 中 telnet，效果如下图：



一、基于用户名密码认证：

Console：

username xiaot password tang（这是本地用户名密码，你也可以采用 AAA 服务器，关于 AAA 服务器的见我的博客《PacketTracer 5.2 基于 AAA 认证的 Easy VPN 实验》

line con 0

login local

这是你从 console 登入，将会看到如下的提示：

Username: xiaot

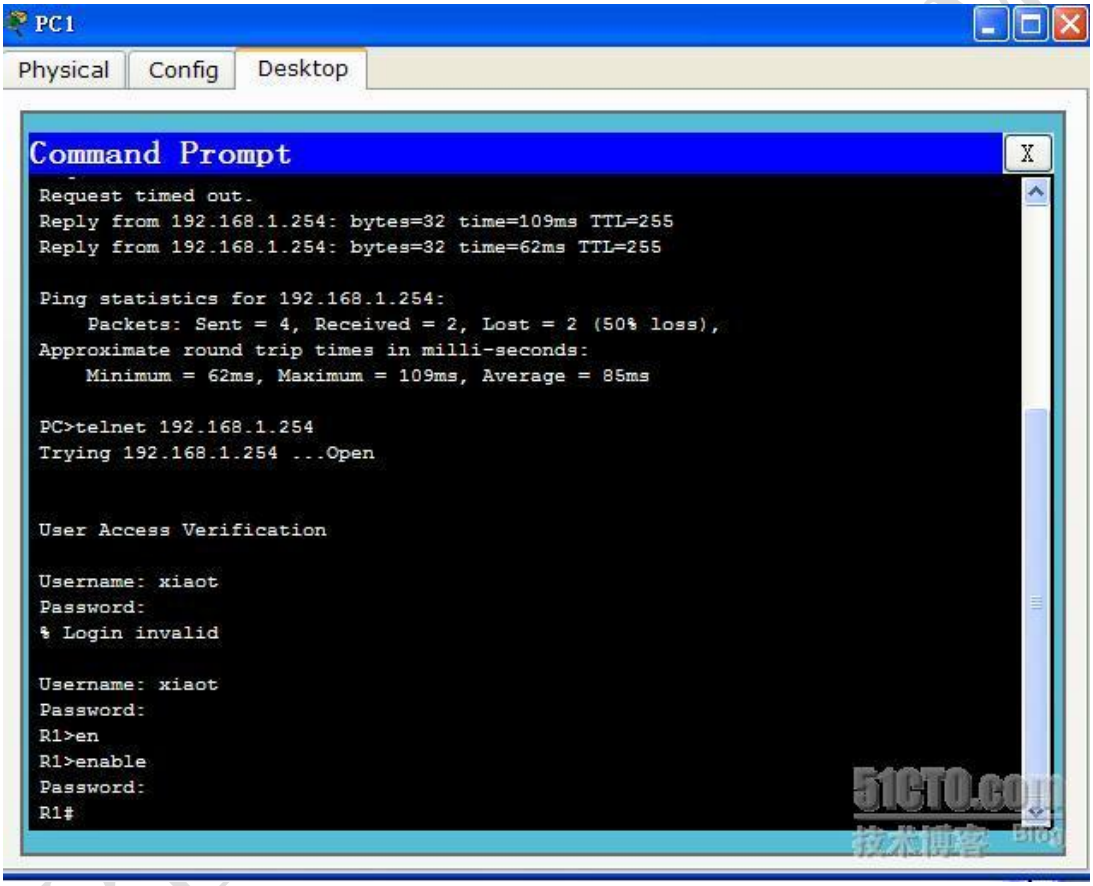
Password:

```
R1>
```

Telnet：

```
username xiaot password  tang
line vty 0 4
login local
enable password 123
```

测试的效果图如下：



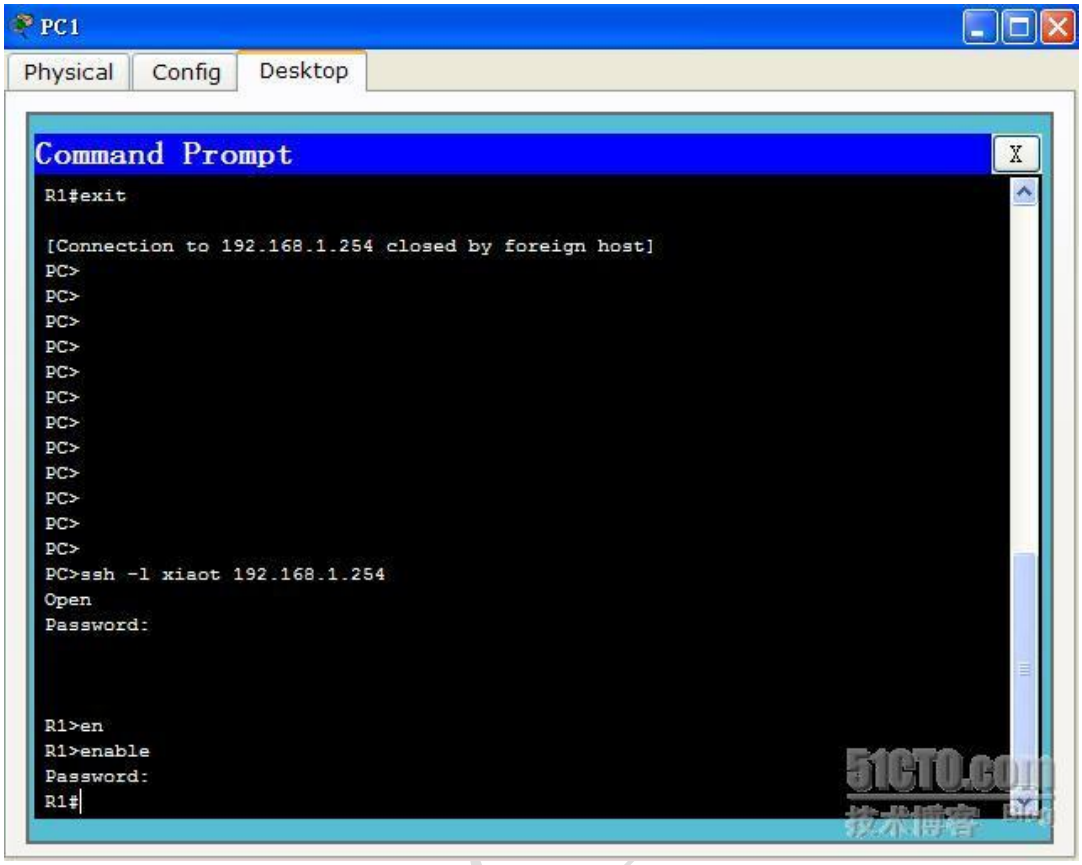
SSH 登入：

```
hostname R1
ip domain-name cicso.com
```

（这两条语句很关键，因为路由要以设备名称和这个域名为材料进行 RSA 算法，产生一对公私密钥对，客户机 SSH 登入时，路由器会将公钥发给客户机，客户机用公钥加密，路由器用私钥解密）

```
crypto key generate rsa
The name for the keys will be: R1.cicso.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]: （产生密钥对的长度）
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
*?? 1 1:35:20.548: %SSH-5-ENABLED: SSH 1.99 has been enabled（当出现这个提示的 SSH 服务也随之开启了！）
line vty 0 4
 login local
 transport input ssh
enable password 123
```

SSH 的测试结果如下：



接下来，我们开始对网络的设备的 IOS，及配置文件备份。IOS 的备份还原在我的博客一文中《PacketTracer 5.2 之路由器 IOS 升级实验指南》有说明，还原的命令跟升级的是一样的。那么备份的命令如下：

```
R1#show flash: （先查看我们需要备份的 IOS）
System flash directory:
File  Length    Name/status
  3   50938004  c2800nm-advipservicesk9-mz.124-15.T1.bin
  2   28282     sigdef-category.xml
  1   227537    sigdef-default.xml
[51193823 bytes used, 12822561 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

R1#copy flash: tftp: （从路由器的 FLASH 中，将文件备份到 tftp 中）
```

Source filename []? c2800nm-advipservicesk9-mz.124-15.T1.bin(原文件)

Address or name of remote host []? 192.168.1.2（TFTP 服务器地址）

Destination filename [c2800nm-advipservicesk9-mz.124-15.T1.bin]?（存放名称，可以自己命名）

.!!

[OK - 50938004 bytes]

50938004 bytes copied in 59.468 secs (856000 bytes/sec)

在 TFTP 服务器中，就可以看到你所备份好的 IOS。配置文件的备份，更 IOS 的备份的思路是一样的。从路由器将 startup-config 或 running-config 备份到 TFTP 服务器上，还原的时候，要千万注意啊，startup-config 还原了，是不需要在保存到路由器，而 running-config 还原了，必须要保存到启动配置文件中。备份和还原命令如下：

R1#copy running-config tftp:

Address or name of remote host []? 192.168.1.2

Destination filename [R1-confg]? running-config（我命名为 running-config，如果不命名这是 R1-confg）

!!

[OK - 686 bytes]

686 bytes copied in 0.125 secs (5000 bytes/sec)

R1#copy startup-config tftp:

Address or name of remote host []? 192.168.1.2

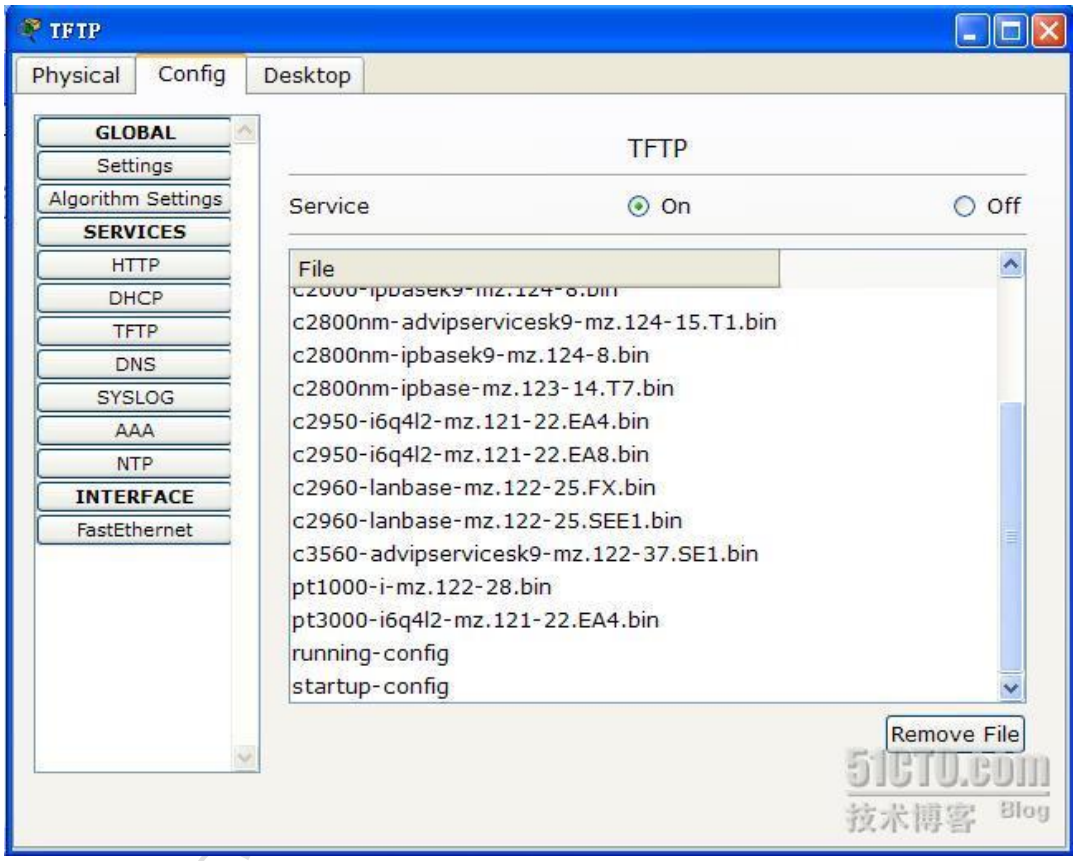
Destination filename [R1-confg]? startup-config（我命名为 startup-config，如果不命名这是 R1-confg）

!!

[OK - 684 bytes]

684 bytes copied in 0.11 secs (6000 bytes/sec)

这时在 TFTP 服务器上的备份效果如如图：



还原的配置命令如下：（以 startup-config 为例）

R1#copy tftp: flash:

Address or name of remote host []? 192.168.1.2

Source filename []? startup-config（服务器上的文件名）

Destination filename [startup-config]?（还原到 flash 中名称，可以命名，建议默认）

Accessing tftp://192.168.1.2/startup-config...

Loading startup-config from 192.168.1.2: !

[OK - 684 bytes]

684 bytes copied in 0.062 secs (11032 bytes/sec)

（注意：还原 running-config 后，在使用 copy running-config startup-config 或 write 保存。）

最后，给大家演示的是路由器的密码恢复实验（由于模拟器不支持做交换机的密码恢复，故小 T 我在这给大家描述一下思路）。在前面我说了，只要在 cisco 网络设备启动后，不让它加载 startup-config 文件就可以了。路由器只要修改寄存值，如：0x2102 是默认的加载 startup-config 文件；0x2142 是不加载 startup-config 文件的。演示实验如下：

把电源关了再开一下，模拟器支持电源的开关（《【交流】浅谈 PacketTracer 5.2 模拟器》一文中有说明）。在路由器重启的时候，出现“####”的时候按下 Ctrl+Break 键盘，加入路由器的 ROM 模式，修改寄存值，效果如下：

```
Self decompressing the image :
#############
monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 0x2142
rommon 2 > boot
```

启动后就如见到如下信息，这个信息室询问式配置，我们选择“no”。就进入到了路由器的命令行配置。密码恢复思路是在这里修改密码，再讲当前的 running-config 保存到 startup-config 中，修改寄存值为默认加载的 startup-config 的。

```
Continue with configuration dialog? [yes/no]: no

Router#copy startup-config running-config
R1(config)#enable password 456
R1(config)#config-register 0x2102
R1r#copy running-config startup-config
R1#reload
```

这样就完成了密码恢复，telnet，ssh 的密码，也在这里配置，后保存到 startup-config，修改寄存值，最后重启。

交互机的密码恢复，小 T 我给大家描述下。以 cisco 2950 为例，在重启交换机的时候，按住交换机上的 Modem 键，然后操作命令先后顺序如下：

flash_init（初始化交换机）

load helper（加载帮助文件）

dir flash:（查看 flash 中文件，你会看到 config.text 文件，这就是交换机的启动文件）

rename flash:config.text flash:config.old（重新命个名，这样交换机就不会加载启动文件了）

boot（启动交换机）

Continue with configuration dialog? [yes/no]: no

Switch#rename flash:config.old flash:config.text(将名字改回到启动文件）

Switch#copy flash:config.text system:running-config（讲启动文件加载到当前运行环境）

Switch（config）#enable password xiaot

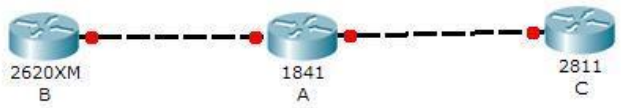
Switch#copy running-config startup-config（修改后的密码保存到启动文件中）

（附件：基本连通的 PKT 文件，大家可以下载实验）

packetTracer 5.2 之 CDP 实验指南

今天小 T 我给大家演示的是 CDP 协议的实验，CDP（cisco Discovery protocol）是 cisco 私有的，专门用来发现邻居的协议。CDP 不像路由协议那样为所有知道的网络显示下一跳目标端口，CDP 只显示直接相连的邻居信息，CDP 非常有助于验证一台路由器是否连在它邻居的适当接口上。简单的讲，通过 CDP 协议能判断网络设备接口是否根据网络拓扑正确连接了！通过 CDP 协议，网络设备能够得知与它相连接的邻居端口和主机名信息。也可以得知一些附加信息如：邻居的硬件模式号码及其功能。CDP 虽然在网络设备调试中，没什么大的作用，但它在排错的时候，也发挥一下它的功能，而且 CDP 协议只使用于 cisco 产品中！

实验拓扑图如下：



IP 的规划如下：

路由器 B：fa0/0 10.1.1.1/24

路由器 A：fa0/0 10.1.1.2/24

fa0/1 172.16.1.1/24

路由器 C：fa 0/1 172.16.1.2/24

网络连通性是由静态路由解决的，三台路由器的配置代码如下：

路由器 B：

```
hostname B
interface FastEthernet0/0
 ip address 10.1.1.2 255.255.255.0

ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

路由器 A：

```
hostname A
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
```

路由器 C：

```
hostname C
interface FastEthernet0/1
 ip address 172.16.1.2 255.255.255.0
ip route 0.0.0.0 0.0.0.0 172.16.1.1
```

现在开始的我们的 CDP 实验，其实 cisco 的 CDP 默认就是开启的，不需要我们特意去配置些什么。cdp enable 是在接口模式下开启 cpd，如果你想让一个特定的接口开启 cpd 而其他接口不开启 cpd 的时候，就用这条命令（注：先要关闭全局默认的 CDP，再搞接口开启）。；cdp run 在全局模式下配置，这条命令一旦敲上去，所有接口都会开启 CDP 功能，这条命令是 cisco 默认开启的。关闭 CDP 命令就是在这两条语句前加个“no”！

我们用 show cdp neighbors 来查看三台路由器的通过 CDP 协议学到了那些邻居信息。显示结果如下：

```
B#show cd neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
```

```
                    S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce    Holdtme    Capability    Platform    Port ID
A             Fas 0/0          171            R         C1841       Fas 0/0

A#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                    S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce    Holdtme    Capability    Platform    Port ID
B             Fas 0/0          135            R         C2600       Fas 0/0
C             Fas 0/1          142            R         C2800       Fas 0/1

C#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                    S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID     Local Intrfce    Holdtme    Capability    Platform    Port ID
A             Fas 0/1          125            R         C1841       Fas 0/1
```

现在就上面得一些信息进行分析一下。Device ID 指的是邻居的名称，也就是在上面配置的 hostname 名字，Local Interfce 是本地的接口，Holdtme 是保持时间，默认是 180 秒，假如我们把路由器 B 与 A 断开，要等 Holdtme 的数字变成零才会删除掉对方的信息。Capability 是现实对方的网络设备是什么设备，R 是路由器，在上面的 Capability Codes 中讲述了字母相对应的意思。Platform 是邻居的网络设备的型号。Port ID 是对方的端口，通过 Port ID 和 Local Interfce 的信息，我们就能知道这台设备的哪个接口与对方的哪个接口连接了。在实际的网络排错中，我们排错的开始第一步是，检查物理连接是否断了，是否接错了接口。通过 CDP 协议，我们就不必跑到设备面前一个一个的排查了！

关于 CDP 的其他命令，我就不多讲了，给他家大致的描述一下。Cdp timer：本命令设置路由器发送 CDP 更新数据的间隔，缺省设置为 60 秒，全局模式下配置。clear cdp table：用于清除路由器的 CDP 表，而一旦清除，在用 show cdp

neighbor 命令不会显示任何信息，直到从一台相邻的路由器收到一 CDP 更新数据包，特权模式下配置。Show cdp interface:本命令显示各端口的 CDP 状态，是特权级别可执行命令。show cdp traffic：本命令将显示路由器已发送和接受了多少 CDP 报文，也显示收到了多少错误的 CDP 报文，运行在特权模式。debug cdp [packets][ip][adjacency][events]:cdp 的调试信息。

PacketTracer 5.2 之 SNMP 实验指南

“十一”八天长假放完了，舒舒服服的睡了好几天觉，饱饱的吃了几顿好的。总算把这几个月上班所消耗的精力和能量补回来了。当然，小 T 我也没放下技术的研究，利用“十一”玩耍期间空余的时间稍微研究了下 PacketTracer 5.2 的 SNMP 实验指南。总算见识到了 SNMP 的功能强大之处，和 SNMP 这个协议复杂程度。说起对 SNMP 了解程度，小 T 我也只了解了 SNMP 的 20%的内容，而且用 PT 来做 SNMP 的实验功能又有限，写的不好还请各位高手和网友指正。

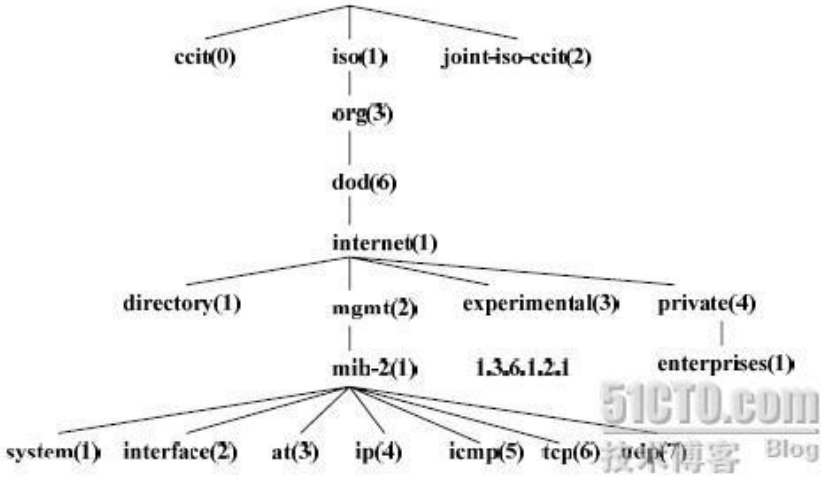
在较小的网络中，网络设备比较少的情况我们常常是用 Telnet，SSH，或者 Web 等方法对网络设备进行维护和监控。但随着网络的规模的逐渐增大，网络设备的数量成级增加，网络管理员很难及时监控所有设备的状态，发现并修复故障；网络设备也可能来自不同的厂商，有的厂商配置设备是命令行，有的是 Web 的，有的是客户端的等等，这些将是网络管理变得更加复杂。在这种情况下，SNMP 的功能就发挥了。

关于 SNMP 详细的原理，大家可以查阅 TCP/IP 协议之类的书。（小 T 我也只弄懂了 20%左右）。我们在 PC 上装上一个网络管理软件（像 cisco 的 cisco network，Windows server 自带的网络管理管理软件等等）做网络管理站，那么网络设备就是我们的被管理对象，网络管理软件与网络设备的之间的通信就是用到了 SNMP 协议，通过 SNMP 协议我们可以获得网络设备系统名，网络配置情况，物理接口状态等等；通过 SNMP 协议我们可以用网络管理软件对网络设备进行配置；通过 SNMP 协议当网络发生了问题时，网络设备通过 SNMP 及时反馈到网络管理站，网络管理员就能第一时间知道网络出问题了。

网管软件是如何通过 SNMP 来实现监控和配置网络设备呢？小 T 我个人理解是（有问题还请大家指点）：用网络管理软件来获得、配置、监控网络设备，其实就对网络设备的数据库的获取、配置、监控。这种数据库就是 MIB（管理信息数据库）。在网络管理软件中也有和网络设备相对的 MIB，可能不同厂商的对标准的 MIB 数据库做了一定“私有化”，只要弄到这些私有 MIB 导入到网络管理软件，我们就能配置管理网络设备。当网络管理站（也就是装了网络管理软件的 PC）对自己的 MIB（与被操作网络设备 MIB 一致）进行操作（如 Get 获取网络设备的信息，Set 修改网络设备配置），产生的应用数据通过 SNMP 协议传递。数

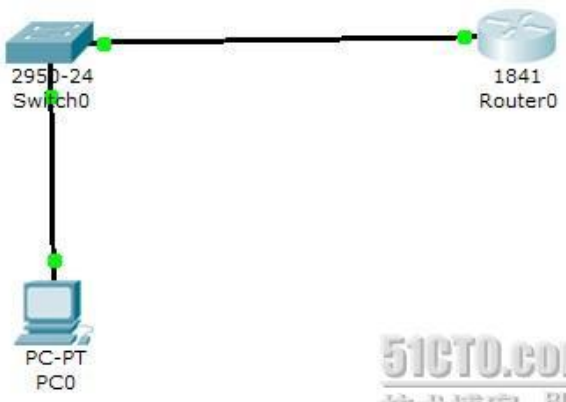
据按 IOS 的七层自上而下的封装数据，数据到达被管理的网络设备解封数据包，最终查看到是 SNMP 数据包，根据数据包里的命令网络设备对自己的 MIB 进行操作（如：将自己的设备信息发送给网络管理站，根据命令对自己 MIB 配置操作到达修改配置的效果）。

由此可见 MIB 是多么的重要的，小 T 我给大家简单讲解下 MIB。MIB 是一种数据库，它存放了网络设备的各种信息，如系统命令信息，配置信息，接口状态信息，路由信息等等。MIB 是以树状结构进行存储的，树的节点表示就是被管理的对象（如：网络设备的接口信息等），也就说我们要对 MIB 进行操作就必须在这个树状的数据存贮结构中找到所要管理信息的位置，在 MIB 中从根开始到节点的唯一路径，我们成为 OID（对象标识符）。如下图简单说明下：



如果我们要获得网络设备的系统信息，那么在操作 MIB 时，它查找的数节点路劲是 1.3.6.1.2.1.1（或者用 iso.org.dod.internet.mgmt.mib-2.system），只要对这个节点信息进行操作就可了。（关于这些节点信息的含义参考 TPC/IP 协议书籍，太多了，小 T 我自己还都没全弄明白）。

关于 SNMP 的一些内容，小 T 我就讲到这里，SNMP 的内容真的是博大精深啊！有兴趣的朋友可以多研究研究，到时候记得告小 T 我哦！现在正式开始今天的 packetTracer 5.2 的 SNMP 实验。网络拓扑图如下：



IP 规划：

路由器：fa0/0 192.168.1.1/24

交换机管理地址：VLAN 1 192.168.1.2/24

PC:192.168.1.10/24

网络设备配置

路由器：

```
hostname R1
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
no shut
```

snmp-server community xiaoro RO（开启 SNMP，community 是一中简单的身份认真，ro 是只读文件，rw 是可读可写文件）

```
snmp-server community xiaorw RW
```

交换机：

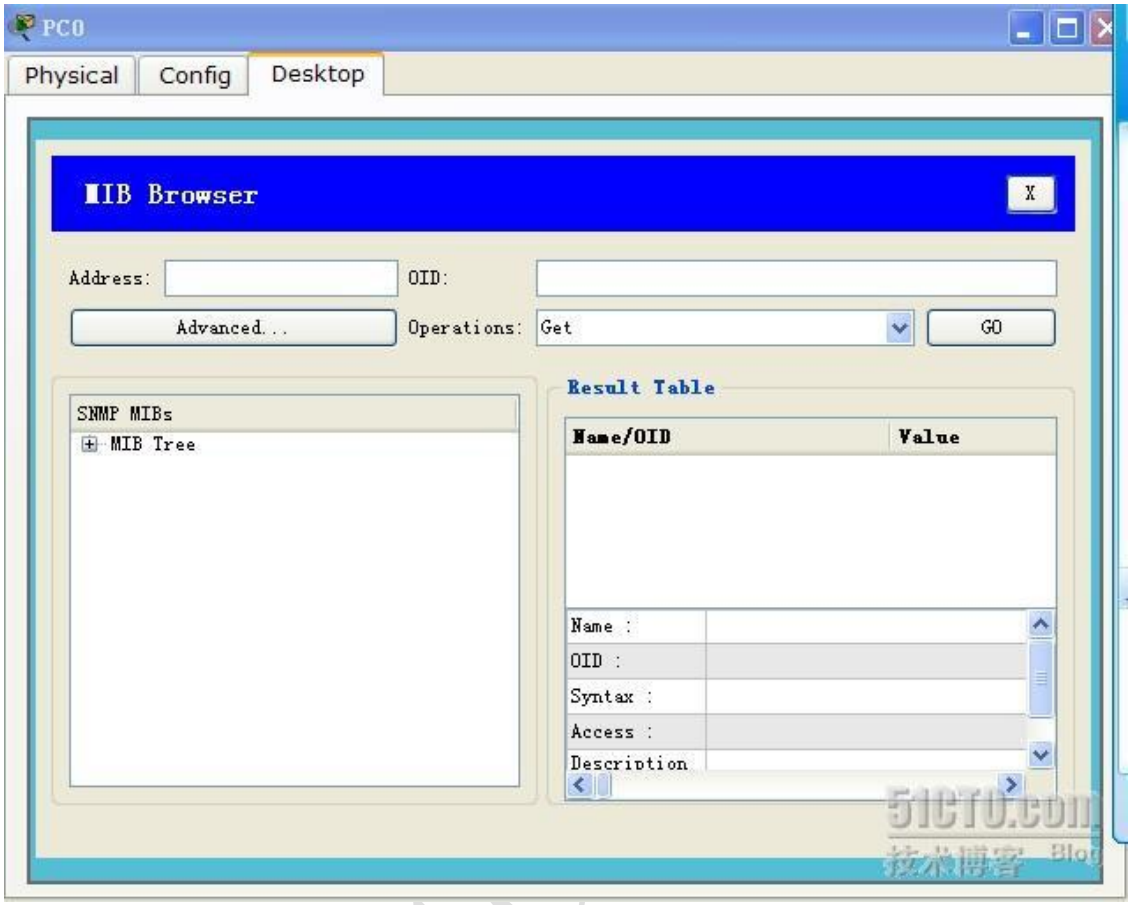
```
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
```

```
snmp-server community xiaoso RO
```

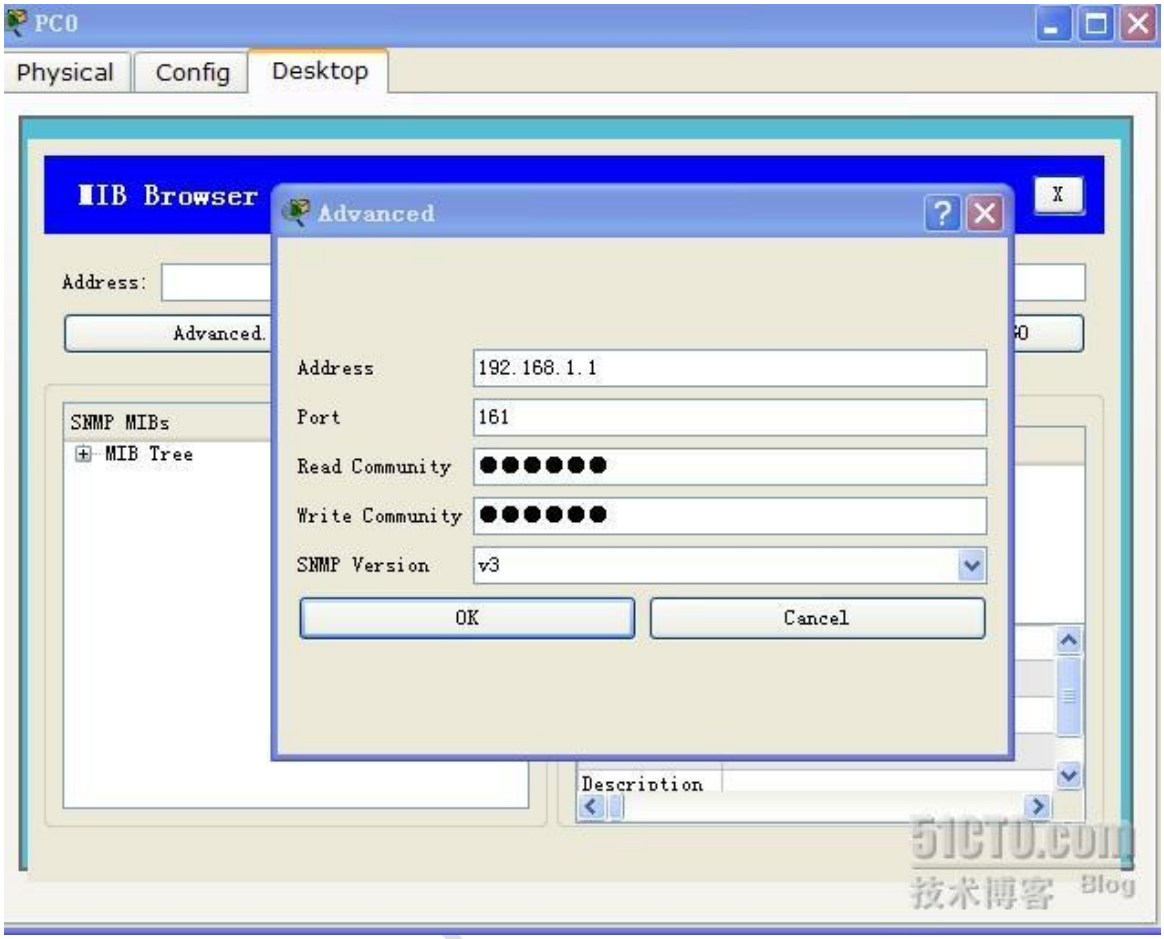
```
snmp-server community xiaosw RW
```

由于的 PT 的的功能有限，小 T 我就演示如何获取网络设备的系统信息和通过 SNMP 来修改网络设备的名字。操作如下：

首先，点进 PC，选着 Destop 的中 MIB(packetTracer 5.2 的一个亮点之一)。

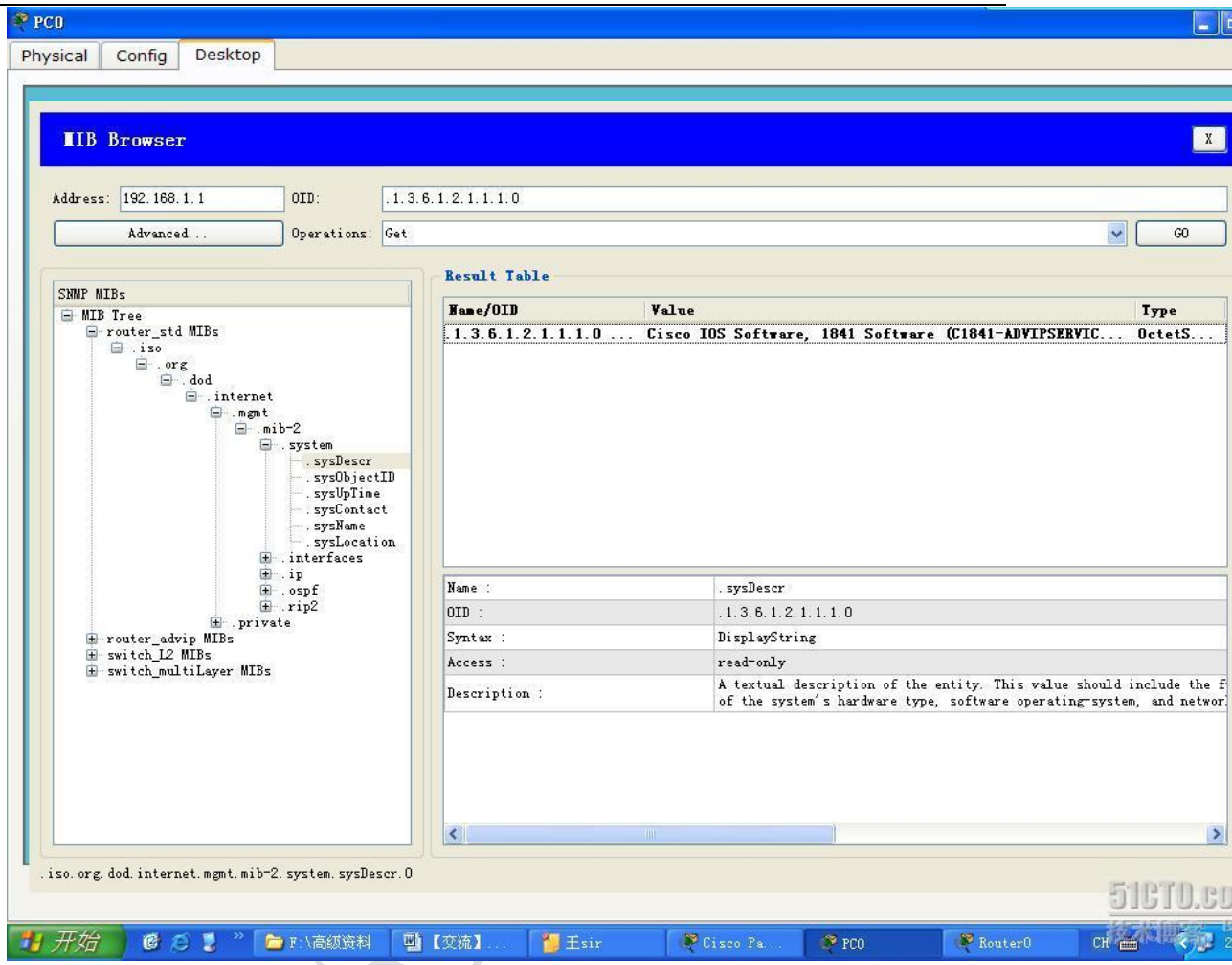


上图就是 MIB 的窗口，网络管理软件中的 MIB 跟上图左下角的 SNMP Tree 差不多，OID 就是 MIB 的信息节点精确路径，operations 就是对 MIB 的操作然后通过 SNMP 传递到网络设备上。首先，选者 Advanced，填入需要管理网络设备的 IP 地址，填入设备上 community 值，这是网络设备与网络管理设备身份认证。如图：



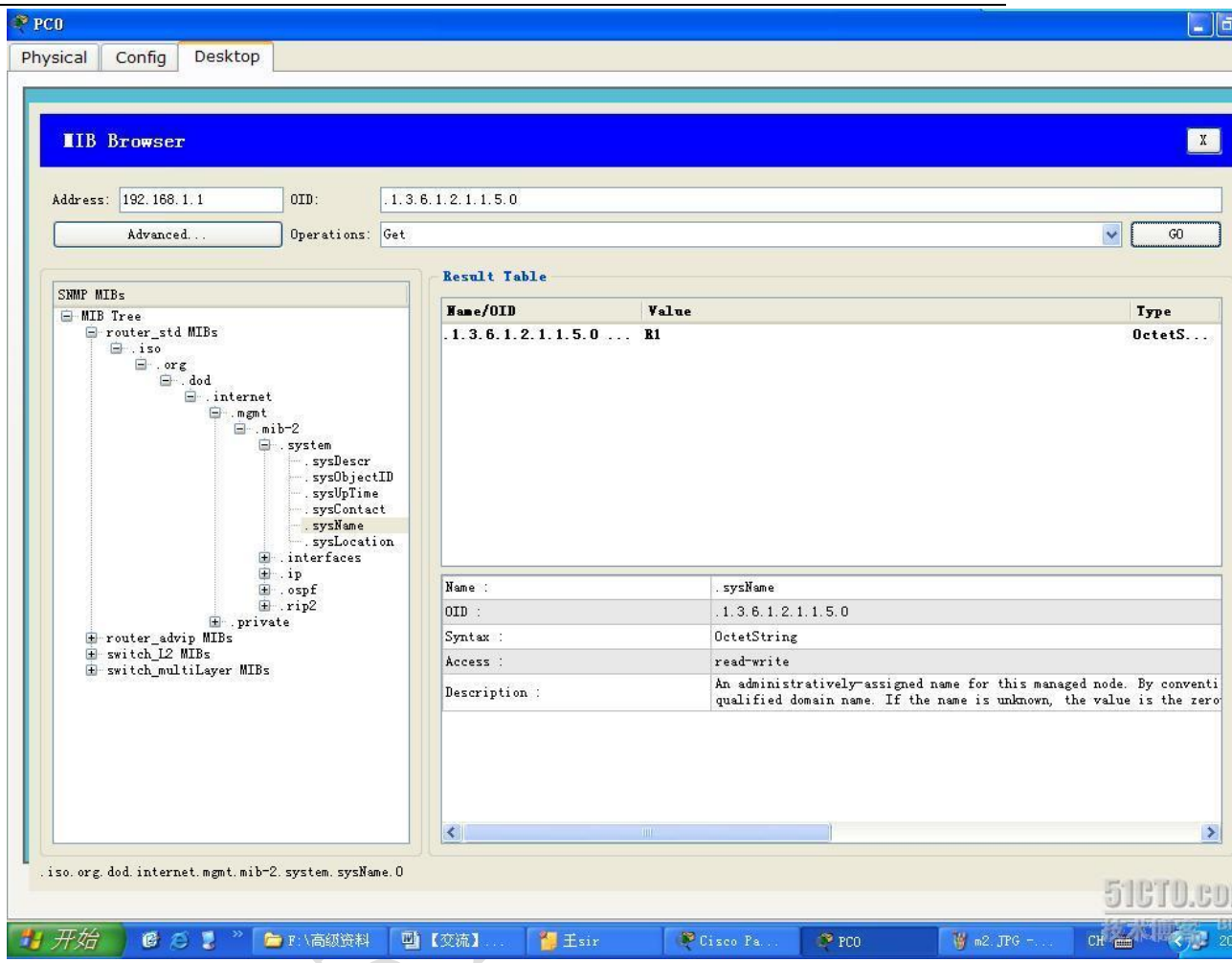
这是路由器的管理 IP，read community 是 xiaoro,write community 是 xiaorw

我们通过查找 MIB 数据库中精确查找我们需要的信息节点路径，在通过 Get 操作以 SNMP 数据到网络设备获取网络设备的信息。如下图，在左下角的 MIB 中找到相应的节点路径（OID：.1.3.6.1.2.1.1.0 或者 iso.org.dod.interface.mgmt.mib-2.system.sysDescr），执行 Get 操作，所获得到的路由器的系统信息描述信息，包括了路由器的型号和 IOS 型号等。

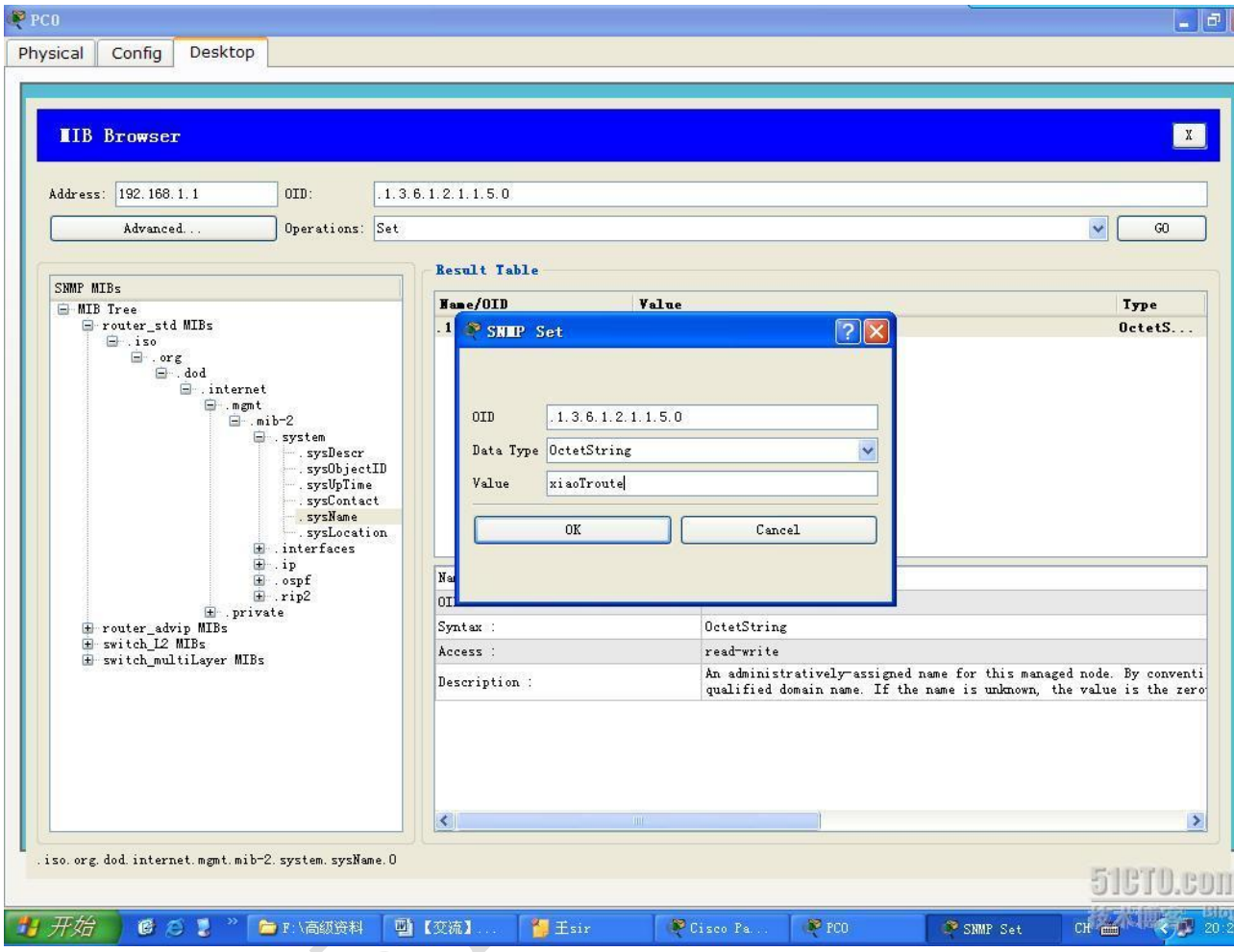


注意：在右下角的方框中显示了 read-only，说明该信息是只读信息，不能通过 SNMP 来配置网络设备。只有 write-read 就可配置。

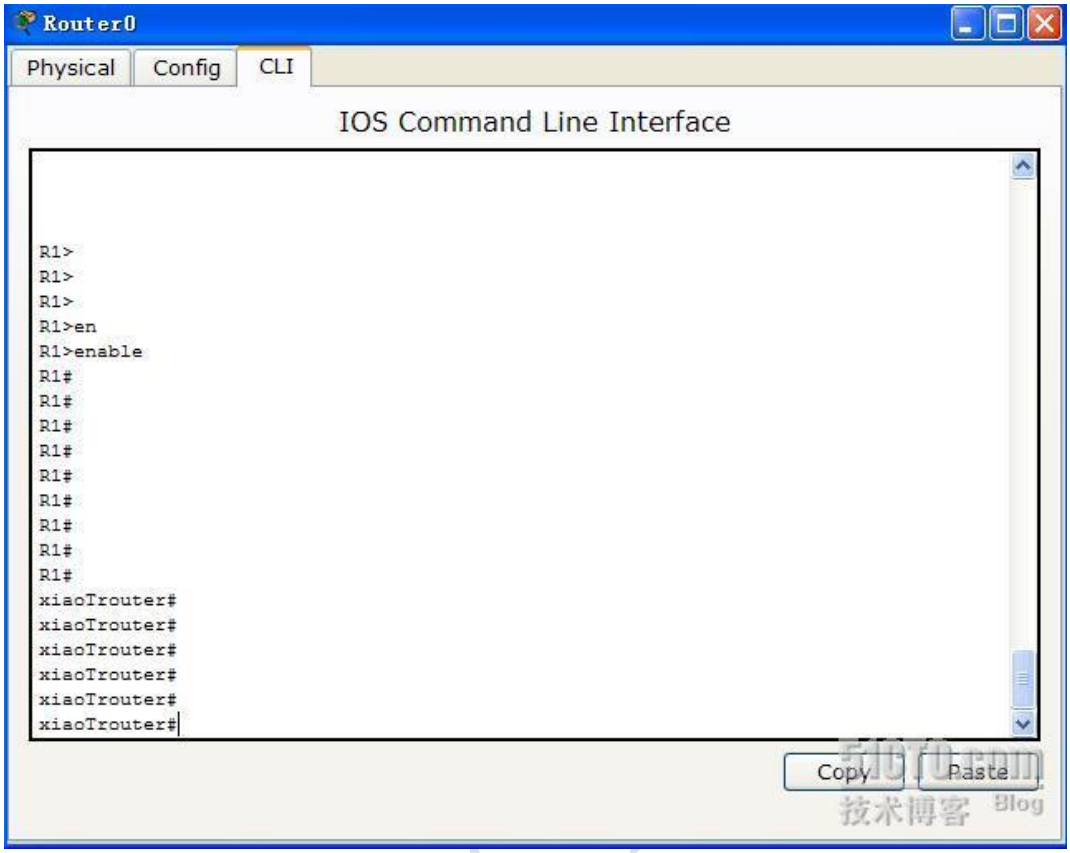
接下来，演示通过 SNMP 来配置网络的 hostname（哎。。PT 功能有限，小 T 我能力有限，通过 SNMP 来配置网络设备在 PT 中只有 hostname 我成功了。如果有高手知道，还请指点啊）。同样，我们上面一样先获取方法一样，我们要找到 MIB 中 sysname 的位置，先获取网络设备的 hostname，效果如下图：



我们看到他的值跟路由上命名是一样的。现在我们来修改一下网络设备的 hostname，把 R1 改成 xiaoTrouter。如图操作：



将 operations 改为 set,然后所要 OID 位置，数据类型是字符串的（SNMP 在表示层用的 ASN.1 抽象语法表示，Value 就是我们要修改的值 xiaoTrouter，然后点击 OK，再点击 GO。我们再路由器上看看，在路由器的命令行中敲几个回车你就看到效果了。如下图：



在通过 PC 上 MIB 来获取路由的 sysname 就可以看到是 xiaoTrouter 了。

PT 的 SNMP 实验演示到这了，交换机的实验就交给大家慢慢研究了。如果，大家想完成更真实的 SNMP 实验，推荐下载 SNMPc7.0 软件和工大瑞普，小凡等模拟器搭建实验环境，效果很爽的。

补充点 PT 中用的到 MIB 知识：

System:这个属性描述网络设备名字，位置等。

If：网络设备接口号，物理地址等

At：有关 ARP 信息。

IP：IP 地址和路由表等信息。

OSPF：OSPF 的相关信息。

RIP2：rip 协议的相关信息。

Private：cisco 私有的 MIB 信息节点。惭愧，小 T 我还没弄明白。

SNMP 的内容真的是博大精深啊，今天的实验还只是些皮毛，小 T 的领悟有限，还有更多对 SNMP 熟悉的朋友指点。博客首页有的我的 QQ 号，大家相互交流下哦！

附件中有本实验的 PKT 文件。http://9916376.blog.51cto.com/468239/210637

一道 CCIE 实验题

前言：

在技术圈中看到这道 IE 实验题(http://g.51cto.com/ciscotest/54780)，对自学 MPLS VPN 刚刚才入门的我，在看到这 IE 的实验题，涉及了 IS-IS，OSPF，BGP，MPLS 和 MPSL VPN 等综合，心中不产生试一试的念头。在细细品味这道 IE 实验的时候，对我最大的难题就是 MPLS VPN 的跨区域（多个 ISP）的实现。这两个星期以来，一直在研究跨域的 MPLS VPN 实验问题，上网查找了 MPLS VPN 跨域方面的资料，无奈大多数资料就一张图一个配置，没有什么详细的说明或者是一个思路。最后，在我自己搜集的 80 多个 G 资料库中，找到一个不错的跨域 MPLS VPN 资料《MPLS Configuration on Cisco IOS Software》，这本书很纤细的讲述了关于 MPLS 配置，无奈全英文的，不得不用那个翻译的牛头不对马嘴的金山快译看，总算或多或少的明白了什么是 MPLS VPN 的 Option A、Option B、Option C 等的意思。为了完成这道 IE 实验题，由于小 T 我的电脑 CPU 还是奔 4 3.0、内存只有 512M，为了节省 CPU 和内存资源，我搜索能达到这次实验要求又能节省资源的 IOS，感谢网友艾文送给我一个 cisco IOS 搜索软件，让我轻松的找找了这次试验我想要的 IOS（c2691-jk9o3s-mz.122-15.T17.bin，支持 MPLS VPN，标签分发协议是 LDP 的，还支持做 IPSec VPN 等等），虽然找到了自己的想要的 IOS，但在做实验的时候，协议开启后，我的电脑嗡嗡的响个不停，可以说，为了完成这次试验，我的电脑在极限操作了。小 T 我并不是什么网络高手，所以，在跟交流这道 IE 实验题的时候，难免有出错的，说的不好处，还请大家指点批评。

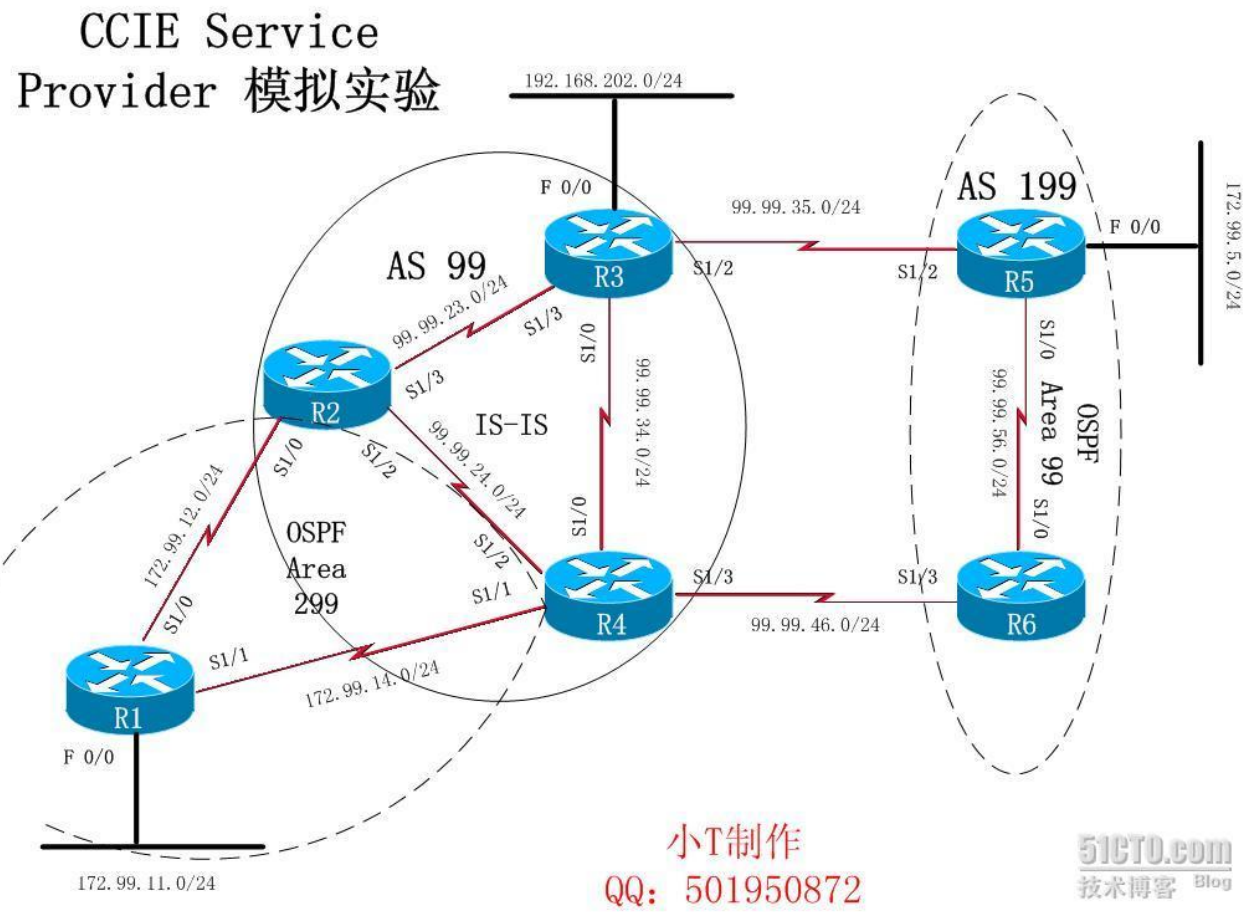
在开始讲述今天的实验之前，首先说明一下，我做的这道 IE 实验题（http://g.51cto.com/ciscotest/54780），我只完成了 85%左右,还有些细节方面，我简单描述下方法，但整体框架已经全部通了，还请大家跟小 T 我一起交流探讨一下。

现在，先聊聊 MPLS VPN，已经学习了 Ipsec VPN，PPTP，l2tp，SSL VPN，Easy VPN 等 VPN 技术，MPLS VPN 的给我的感觉有点像是虚拟防火墙似的，在一个

物理设备逻辑成几个设备，那么 MPLS VPN 则是在各个 PE 路由器上，虚拟出了多张虚拟路由表，每个路由表都是独立，相互不影响，也就说，一台 PE 路由上有公网的路由表和私网的路由表，那么我们私网的路由表的路由在公网路由表中是看不见得，同样公网路由表中的路由在私网路由表上也是看不到的、简单点我们可以想象成一个路由器就变成了多个路由器，路由选路都是根据自己的路由表路由。

在讲述本次试验的时候，先申明下，小 T 我做的只是个参考配置，跟原题有微弱的差别，但大致还是相同的。本次试验，涉及的技术原理太多，不好一一在这讲述，本次试验重点简述的我的配置过程。在实际工程中也是一样，都是一步一步的完成配置，这样做的好处是确保出错率降到最低。

首先，是实验的网络拓扑图：



根据题意（http://g.51cto.com/ciscotest/54780）分析，在本次试验中，R1 是 CE，R2、R3、R4、R5 即是 PE 也是 P，R6 是 P（P 是核心路由器，它要具备

传递 VPNv4 的路由，就说 PE 之间存在 P 设备，那么 PE 的 VPNv4 路由被 P 设备所传递，否侧 PE 不能相互学习到路由）。题目要求 R1、R3、R5 的通过 MPLS VPN，让 172.99.11.0/24、192.168.202.0/24、172.99.5.0/24 这些私网能够相互通信。简单的描述一下，数据过程，以 R1 到 R5 的过程，R1 的 172.99.11.0/24 到 172.99.5.0/24，首先，数据进入 R1，由于 R1 是 CE，那么数据就跟普通的路由器一样选择到目标网络的路由（由于题目要求，R1←-→R2.R2←→R3，R3←→R5 主链路），数据进入到 R2，由于 R2 和 R1 相连的接口加入到了虚拟路由转发表中，那么数据是不会走真实的路由，走的是虚拟路由，根据数据的封装，IP 包被私网标签封装，再被公网标签封装，在 MPLS 设备中，在没到达目标方的 PE，都是公网标签进行交换变更。到达目标 PE 时，去除公网标签，在取出私网标签，数据以更具虚拟路由转发表，从相应的接口出去，之后就是普通的 IP 包了！

以下，是实验的 IP 规划：

loopback:

R1:99.99.0.1 255.255.255.255

R2:99.99.0.2 255.255.255.255

R3:99.99.0.3 255.255.255.255

R4:99.99.0.4 255.255.255.255

R5:99.99.0.5 255.255.255.255

R6:99.99.0.6 255.255.255.255

链路 IP：

R1<--->R2

R1 172.99.12.1 255.255.255.0

R2 172.99.12.2 255.255.255.0

to YW

R1 172.99.11.1 255.255.255.0

R1<--->R4

R1 172.99.14.1 255.255.255.0

R4 172.99.14.2 255.255.255.0

R2<--->R4

R2 99.99.24.1 255.255.255.0

R4 99.99.24.2 255.255.255.0

R2<--->R3

R2 99.99.23.1 255.255.255.0

R3 99.99.23.2 255.255.255.0

R3<--->R4

R3 99.99.34.1 255.255.255.0

R4 99.99.34.2 255.255.255.0

to YW

R3 192.168.202.1 255.255.255.0

R3<--->R5

R3 99.99.35.1 255.255.255.0

R5 99.99.35.2 255.255.255.0

R4<--->R6

R6 99.99.46.2 255.255.255.0

R4 99.99.46.1 255.255.255.0

R5<--->R6

R5 99.99.56.1 255.255.255.0

R6 99.99.56.2 255.255.255.0

to YW

R5 172.99.5.1 255.255.255.0

本次实验步骤：

一， 基本连通的性的配置（注：小 T 我在附件中共享了详细配置步骤，这里我只简单的描述一些注意事项和重点）。不管是在做实验，还是在做工程，这一步是最基本，但又是常常被大家所忽视的。很多人配置好了 IP 就马上开始，出问题，排查了很久，最好猜发现时 IP 地址错了。所以，小 T 我特别强调，这一步很重要，在配置好 IP 后，先 Ping 一下直接的 IP 是否通了，在确定 IP 没错再开始下一步。

二， IGP 基本连通配置，在这一步配置我们常见的 IGP 协议，如：RIP，IS-IS，OSPF 等等，让 AS 中路由器都学到路由。在这一步要检查好路由是否学到了。

三， 开启 MPLS。让 AS 内的路由分发和学习标签，这就公网标签。

四， BGP 配置。配置好 EBGP 和 IEBGP 邻居，根据需求让不同 AS 间学习到对方 AS 的 BGP 路由。

五， 配置 MP-BGP。让 MP-IBGP 和 MP-EBGP 邻居建立起来。MP-GBP 协议用来传递和学习 VPNv4 路由。

六， 在 PE 上创建 VRF（虚拟路由转发表），将与 CE 相连的接口加入到相应的 VRF 中。在 PE 上，将 VRF 路由重发布到与 CE 相同的协议中，CE 的路由重发布到 VRF 中。

七， CE 的路由配置。跟我平时的普通路由配置是一样的。最后他会学到目标死网的路由。

部分实验命令简单解释，详细的还请大家到网络查资料。

ip cef （开启 cisco 的 cef 转发）

mpls label protocol ldp （MPLS 的标签协议选择为 ldp，cisco 私有的为 tdp）

int s1/3

mpls ip（接口开启 MPLS）

mpls mtu 1520（由于 MPLS VPN 的数据包大于了 1500，故设置为 1520）

router bgp 99

no bgp default route-target filter（在 MP-EGBP 中，若不关闭，则无法传递 VPNv4 路由）

address-family vpnv4（VPNv4 地址族配置）

neighbor 99.99.0.2 activate（激活 MP-GBP 的 MP-IBGP 邻居）

neighbor 99.99.0.2 send-community extended（发送团体属性支持 VPNv4 路由的传递）

neighbor 99.99.0.2 next-hop-self（下一跳指向自己）

neighbor 99.99.35.2 activate（激活 MP-GBP 的 MP-EBGP 邻居）

neighbor 99.99.35.2 next-hop-self

ip vrf xiaot（创建虚拟转发表）

rd 1:110（路由区分符）

route-target export 2:110（路由目标传出标识）

route-target import 2:110（路由目标接受标识）

exit

int s 1/1

ip vrf forwarding xiaot（标定 VRF）

ip add 172.99.14.2 255.255.255.0

no shut

exit

router ospf 299 vrf xiaot（在 VRF 中运行与 CE 相同的路由协议，这是 OSPF，其他协议有所不同，大家查阅资料）

router-id 99.99.0.2

network 99.99.0.4 0.0.0.0 area 0

network 172.99.12.0 0.0.0.255 area 0

redistribute bgp 99 metric 1000 metric-type 1 subnets（将通 BGP 学到的路由重发到 ospf 路由中来）。

router bgp 99

address-family ipv4 vrf xiaot(选择在路由协议内为每个 VRF 进程配置)

redistribute ospf 299 metric 1000 match internal external 1 external 2(将 OSPF 重发布道 BGP 中)

测试结果：（简单举例，详细的测试结果在附件中共享）

R2、R3、R4 的 IS-IS 邻居关系

```
R2#show clns neighbors
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R3             Se1/3       *HDLC*          Up     25        L1   IS-IS
R4             Se1/2       *HDLC*          Up     21        L1   IS-IS

R3#show clns neighbors
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R4             Se1/0       *HDLC*          Up     20        L2   IS-IS
R2             Se1/3       *HDLC*          Up     29        L1   IS-IS

R4#show clns neighbors
```

```
    System Id       Interface   SNPA                State  Holdtime  Type Protoc
ol
    R3              Se1/0       *HDLC*              Up     26        L2   IS-IS
    R2              Se1/2       *HDLC*              Up     27        L1   IS-IS
```

测试结果：

CE 上的情况：

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

    Gateway of last resort is not set

         99.0.0.0/32 is subnetted, 1 subnets
    C       99.99.0.1 is directly connected, Loopback0
         172.99.0.0/24 is subnetted, 4 subnets
    C       172.99.14.0 is directly connected, Serial1/1
    C       172.99.12.0 is directly connected, Serial1/0
    C       172.99.11.0 is directly connected, FastEthernet0/0
    O E1    172.99.5.0 [110/1100] via 172.99.12.2, 00:00:20, Serial1/0
    O E1 192.168.202.0/24 [110/1100] via 172.99.12.2, 00:00:20, Serial1/0
```

（通过 R2 讲 VPNv4 路由重发布进来的）

```
R1#traceroute 172.99.5.1

Type escape sequence to abort.
Tracing the route to 172.99.5.1

  1 172.99.12.2 116 msec 32 msec 16 msec
  2 99.99.35.1 [MPLS: Label 30 Exp 0] 92 msec 156 msec 116 msec
  3 172.99.5.1 212 msec *  284 msec
```

PE 上的信息：

R2#show mpls forwarding-table （公网标签）

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
16	Pop tag	99.99.0.3/32	4230	Se1/3	point2point
17	Pop tag	99.99.0.4/32	3633	Se1/2	point2point
18	Pop tag	99.99.34.0/24	0	Se1/2	point2point
	Pop tag	99.99.34.0/24	0	Se1/3	point2point
22	Untagged	99.99.0.1/32[V]	0	Se1/0	point2point
23	Untagged	172.99.14.0/24[V]	0	Se1/0	point2point
24	Aggregate	172.99.12.0/24[V]	636		

R2#show ip bgp vpnv4 all labels （私网标签）

Network	Next Hop	In label/Out label
Route Distinguisher: 1:110 (xiaot)		
99.99.0.1/32	172.99.12.1	22/nolabel
172.99.5.0/24	99.99.0.3	nolabel/30
172.99.12.0/24	0.0.0.0	24/aggregate(xiaot)

172.99.14.0/24 172.99.12.1 23/nolabel

192.168.202.0 99.99.0.3 nolabel/27

R2#show ip route vrf xiaot（查看虚拟路由转发表）

Routing Table: xiaot

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

99.0.0.0/32 is subnetted, 1 subnets

O 99.99.0.1 [110/101] via 172.99.12.1, 01:23:33, Serial1/0

172.99.0.0/24 is subnetted, 3 subnets

O 172.99.14.0 [110/300] via 172.99.12.1, 01:23:33, Serial1/0

C 172.99.12.0 is directly connected, Serial1/0

B 172.99.5.0 [200/0] via 99.99.0.3, 00:09:55

B 192.168.202.0/24 [200/0] via 99.99.0.3, 00:10:25

（通过 MP-BGP 学到的路由）

R5#ping vrf xiaot 99.99.0.1（在 R5 上测试 MPLS VPN 连通，小 T 我就没再给 R5 做个 CE 了，电脑已经是极限操作了）

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 99.99.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 92/132/164 ms

后语：

本次试验小 T 我只完成了我只完成了 85%左右，还有一点路由过滤和路由优化，就留给大家研究了。通过这次的实验，小 T 我充分的认识到，虽然很多技术都学过了，但还不够深入，原理还不够理解透彻，在做本次试验的时候，查阅前面的知识和自学 MPLS VPN 占了大部分时间。好好自我反省下，调整好自己的心态，重新开启。本次实验，不足之处，太请各位指点批评，小 T 我坚信，技术只有交流才能有更好更快的进步！

欢迎大家常到我博客做客!!!

----------小 T

注：附件中有详细的配置过程 http://9916376.blog.51cto.com/468239/217626

PacketTracer 5.2 的 IPsec VPN 实验说明(附 PacketTracer 5.2 下载地址)

[模拟器解压码：www.renzhengwang.com(无下划线）]
嗨~~
大家好！我是小 T!
本人对交换路由，防火墙，VPN 技术有较好的掌握！了解 MPLS 和 VOIP 的基本原理。
较熟练的玩弄 PacketTracer 工大瑞普和小凡模拟器。愿与大家一起分享探讨网络技术！
我的ＱＱ：501950872

废话就不多说了！现在聊聊 PacketTracer 5.2 这个模拟器的 VPN 实验！（说的不好，还请大家指正）
PacketTracer 5.2 下载地址：(直接点击到迅雷就可以下载了）
ftp://renzhengwang:renzhengwang@www.renzhengwang.com/sim/PacketTracer%205.2_setup.rar

PacketTracer 这款模拟器，虽然比不上工大瑞普和小凡等模拟器，但作为初学者的入门，模拟器是一个不错的模拟器。其优点在于较真实的事物效果功能（能看交换机路由器的形状，能换网络模块等），能加深初学者网络拓扑图的学习。在 PacketTracer 5.2 之前的 PacketTracer 系列模拟器都不能做 VPN 实验。现在 PacketTracer 5.2 可以做 VPN，但功能有限，只能做一部分 VPN 实验，传输模式的 IPSEc VPN 和 easy VPN。（若想玩更深的 VPN，还是会玩工大瑞普和小凡模拟器）。

现在就开始 PacketTracer 5.2 的 IPsec VPN 实验：（附件中 VPN.JPG 是网络拓扑）
网络拓扑大概描述一下：
Router 1 模拟成 Internet 网（其实，就是没有私有 IP 地址路由的路由器，在说通俗点，现在 VPN 技术常用来解决总部与分部跨越 Internet 网解决内部私有地址的连通性）
Router 3 为总部，Router 4 为分部。
IP 规划：
Router 1 FastEthernet0/0 200.1.1.1 FastEthernet0/1 100.1.1.1
Router 3 FastEthernet0/0 192.168.1.254 FastEthernet0/1 100.1.1.2
Router 4 FastEthernet0/0 200.1.1.2 FastEthernet0/1 192.168.2.254
PC1 ： 192.168.1.1/24
PC2: 192.168.2.1/24
实验要求让总部和分布的私有地址能通信！(大家可以按我的配置做一遍，红色为 VPN 配置关键代码，在没配置 VPN 时，PC1 是不能与ＰＣ２ 相互 Ping 通）

配置如下：
Router1 的配置（Internet）：
interface FastEthernet0/0
ip address 200.1.1.1 255.255.255.0
no shutdown

```
interface FastEthernet0/1
ip address 100.1.1.1 255.255.255.0
no shutdown
```

Router 3 的配置：

```
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share

crypto isakmp key tom address 200.1.1.2

crypto ipsec transform-set tim esp-3des esp-md5-hmac

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255


crypto map tom 10 ipsec-isakmp
set peer 200.1.1.2
set transform-set tim
match address 101
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
no shutdown

interface FastEthernet0/1
ip address 100.1.1.2 255.255.255.0
no shutdown
crypto map tom

ip route 0.0.0.0 0.0.0.0 100.1.1.1
```

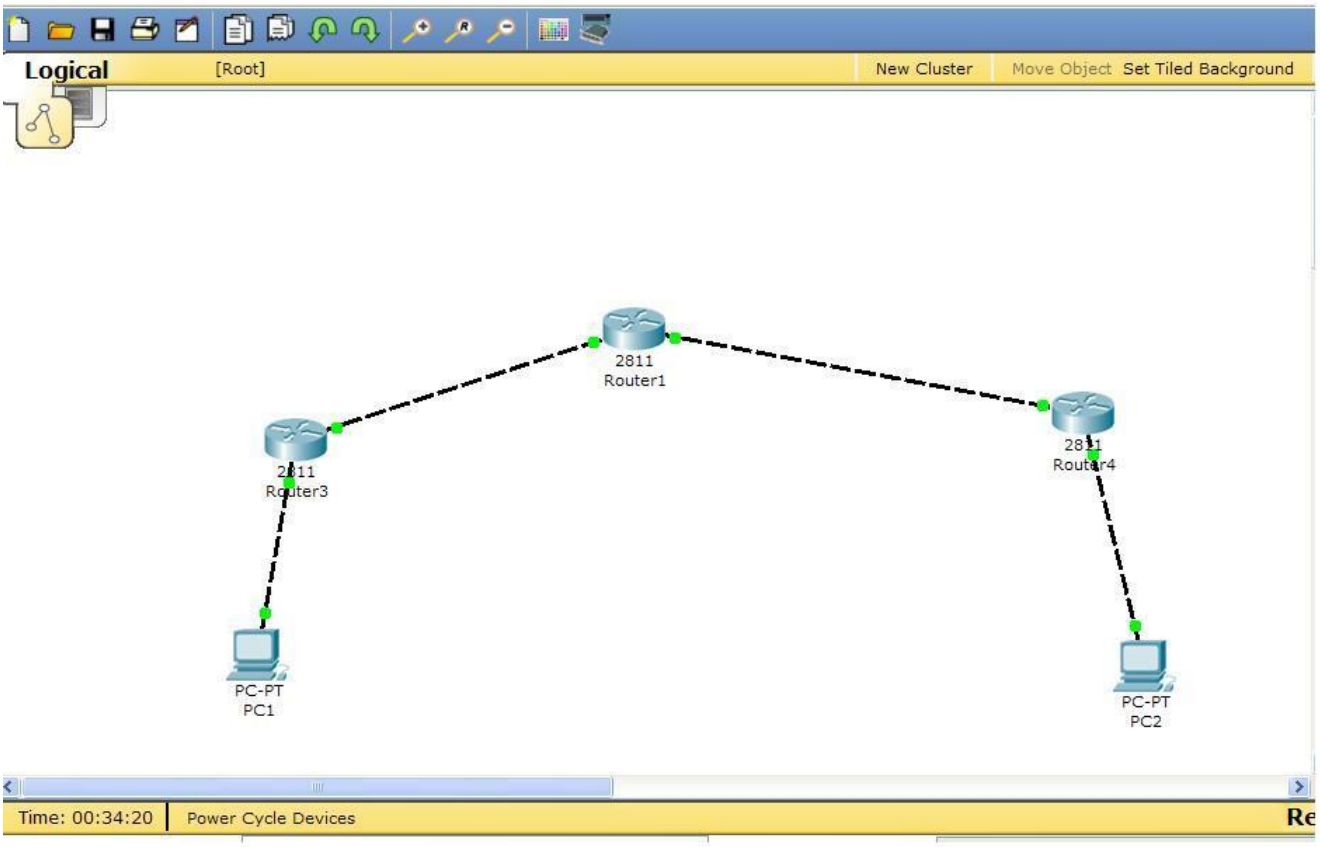
Router 4 的配置：

```
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share

crypto isakmp key tom address 100.1.1.2

crypto ipsec transform-set tim esp-3des esp-md5-hmac
!
crypto map tom 10 ipsec-isakmp
```

```
set peer 100.1.1.2
set transform-set tim
match address 101

access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
interface FastEthernet0/0
ip address 200.1.1.2 255.255.255.0
no shutdown
crypto map tom

interface FastEthernet0/1
ip address 192.168.2.254 255.255.255.0
no shutdown

ip route 0.0.0.0 0.0.0.0 200.1.1.1
```

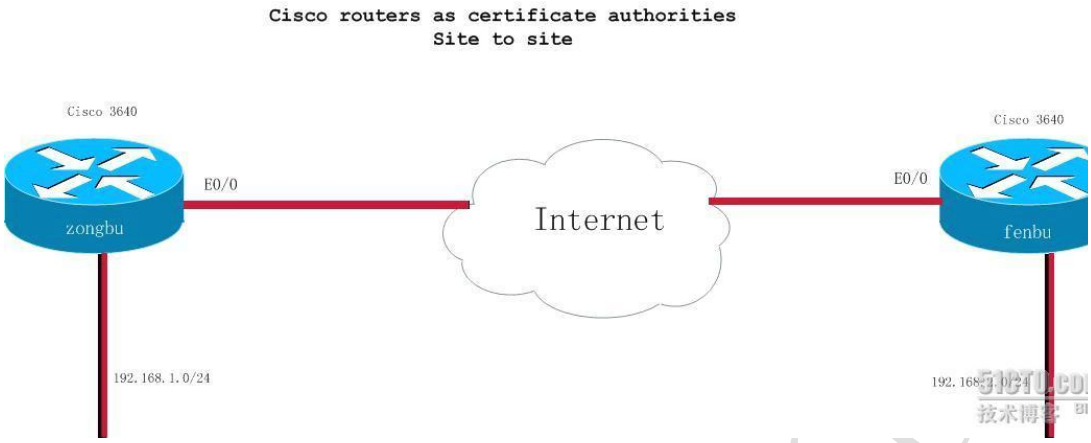
最终，PC1 和 PC 2 能相互 Ping 通。（在 Ping 的过程中，会丢掉几个包，因为在建立 IPSec VPN 的协商）。用 show crypto isakmp sa 和 show crypto ipsec sa 能看到 IPSec VPN 协商好的内容状态。

以上，就是我用 PacketTracer 5.2 做的 VPN 实验！
有什么问题，还请大家指正！
谢谢！！！



本次拓扑图下载:http://9916376.blog.51cto.com/468239/196247

路由器做 CA (数字证书）服务器站点到站点 VPN 实验



这是用工大瑞普模拟器做的关于数字证书的 VPN 实验。小 T 我期待大家的指点。

实验基本思路：

总部的 cisco 3640 路由器作为 ca 服务器，分部向总部请求根证书和自己的设备证书，总部也向自己请求跟证书和自己的设备证书。

2.实验步骤：

总部的基本配置：

```
enable
conf t
hostname zongbu
no ip domain-lookup
line console 0
logging sy
exec-time 0 0
exit
interface ethernet 0/0
ip address dhcp（获取的地址为 200.1.1.2，同时获取一条缺省路由，下一跳 200.1.1.1）
no shut
exit
interface ethernet 0/2
ip address 192.168.1.1 255.255.255.0
no shut
no keepalive
exit
```

分部的基本配置：

```
enable
conf t
hostname fenbu
```

no ip domain-lookup
line console 0
logging sy
exec-time 0 0
exit
interface ethernet 0/0
ip address dhcp（获取的地址为 210.1.1.2，同时获取一条缺省路由，下一跳 210.1.1.1）
no shut
exit
interface ethernet 0/2
ip address 192.168.2.1 255.255.255.0
no shut
no keepalive
exit

总部路由器做 ca 服务器配置
clock set 10:25:00 apr 18 2009
（时间必须配置其分部时间需与总部 ca 时间同步，若时间没配置，总部 ca 服务不能开启。分部时间与总部不同步则获取不到证书）
ip domain-name t31.com
crypto key generate rsa general-keys label lab modulus 1024
ip http server（此服务必须开启）
crypto pki server lab（创建 ca 服务器名字为 lab）
issuer-name CN=zongbu.t31.com,L=changsha,C=CN（填写 ca 服务器的信息）
no shutdown (开启 ca 服务器，并产生根证书)
%Some server settings cannot be changed after CA certificate generation.

% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Re-enter password:
（此提示为输入一个大于 7 字符的密码来保护私钥，是必须的）
% Certificate Server enabled.
（ca 服务开启，若 ca 时间没设置的话，服务是无法开启的）
zongbu#show crypto ca certificates （查看 ca 的根证书）
CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Issuer:
cn=zongbu.t31.com
l=changsha
c=CN

Subject:
cn=zongbu.t31.com
l=changsha
c=CN
Validity Date:
start date: 10:25:41 UTC Apr 18 2009
end date: 10:25:41 UTC Apr 17 2012
Associated Trustpoints: lab

总部自己向自己请求根证书（若总部不先向自己申请根证书，则自己的设备证书是获不到的）
crypto ca trustpoint 200.1.1.2（指点信任点）
enrollment mode ra
enrollment url http://200.1.1.2
exit
crypto ca authenticate 200.1.1.2（请求根证书）
Certificate has the following attributes:
Fingerprint MD5: BA3F31AF 9E701632 D393AC08 36BCC5DD
Fingerprint SHA1: 9EDD4FFF 4F231045 85218C21 8FCDD867 24B2874F
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
crypto ca enroll 200.1.1.2（请求自己的设备证书）
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Apr 18 10:30:53.423: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pai
r
Re-enter password:
% The subject name in the certificate will include: zongbu.t31.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate 200.1.1.2 verbose' command will show the
fingerprint.
Apr 18 10:31:00.143: CRYPTO_PKI: Certificate Request Fingerprint MD5: FF5
49ED7
0F2050DD 712E3CEB AC68AB6F
Apr 18 10:31:00.143: CRYPTO_PKI: Certificate Request Fingerprint SHA1:
784D0FB9 B67FA0BC 8AA900EE BD61A0A8 D1627511

（注：路由器做 ca，证书是手动颁发的，此时证书为挂起状态）

zongbu#crypto pki server lab info requests

（查看 ca 的请求信息，lab 为定义的 ca 服务名称）

Enrollment Request Database:

Subordinate CA certificate requests:

ReqID State Fingerprint SubjectName

RA certificate requests:

ReqID State Fingerprint SubjectName

Router certificates requests:

ReqID State Fingerprint SubjectName

---

1 pending FF549ED70F2050DD712E3CEBAC68AB6F hostname=zongbu.t31.com

（总部的设备证书请求为挂起状态）

zongbu#crypto pki server lab grant all

（为所有证书请求进行颁发，all 是所有，也可用数字，用数字则是请求信息中对应的 ReqID，

等待一分钟左右，证书被颁发下来）

Apr 18 10:35:16.487: %PKI-6-CERTRET: Certificate received from Certificate Authority（获取到证书）

zongbu#show crypto ca certificates

（此时在查看，就有两个证书根证书和总部的设备证书，但注意的是 ca 自己产生的根证书和自己向自己请求的根证书是一样的。）

Certificate

Status: Available

Certificate Serial Number: 02

Certificate Usage: General Purpose

Issuer:

cn=zongbu.t31.com

l=changsha

c=CN

Subject:

Name: zongbu.t31.com

hostname=zongbu.t31.com

Validity Date:

start date: 10:33:44 UTC Apr 18 2009

end date: 10:33:44 UTC Apr 18 2010

Associated Trustpoints: 200.1.1.2

CA Certificate

Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Issuer:
cn=zongbu.t31.com
l=changsha
c=CN
Subject:
cn=zongbu.t31.com
l=changsha
c=CN
Validity Date:
start date: 10:25:41 UTC Apr 18 2009
end date: 10:25:41 UTC Apr 17 2012
Associated Trustpoints: 200.1.1.2 lab

分部路由器配置：
clock set 10:25:00 apr 18 2009
（时间必须配置其分部时间需与总部 ca 时间同步，分部时间与总部不同步则获取不到证书）。
ip domain-name t31.com
crypto key generate rsa general-keys modulus 1024
crypto ca trustpoint 200.1.1.2（指点信任点）
enrollment mode ra
enrollment url http://200.1.1.2
exit
crypto ca authenticate 200.1.1.2（请求根证书）
Certificate has the following attributes:
Fingerprint MD5: BA3F31AF 9E701632 D393AC08 36BCC5DD
Fingerprint SHA1: 9EDD4FFF 4F231045 85218C21 8FCDD867 24B2874F
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
crypto ca enroll 200.1.1.2（请求自己的设备证书）
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: fenbu.t31.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n

Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate 200.1.1.2 verbose' command will show the fingerprint.
Apr 18 10:41:46.151: CRYPTO_PKI: Certificate Request Fingerprint MD5: 8D7E2D33
E1DB8402 1F35D41B 6B3AFB9B
Apr 18 10:41:46.151: CRYPTO_PKI: Certificate Request Fingerprint SHA1: A805BCFD CC113FB2 29FD572A AE1E996B ACC08D4B
（注：路由器做 ca，证书是手动颁发的，此时证书为挂起状态）

zongbu#crypto pki server lab info requests
Enrollment Request Database:
Subordinate CA certificate requests:
ReqID State Fingerprint SubjectName

RA certificate requests:
ReqID State Fingerprint SubjectName

Router certificates requests:
ReqID State Fingerprint SubjectName
---
2 pending 8D7E2D33E1DB84021F35D41B6B3AFB9B hostname=fenbu.t31.com
（分部的设备证书请求为挂起状态）

zongbu#crypto pki server lab grant all
（为所有证书请求进行颁发，all 是所有，也可用数字，用数字则是请求信息中对应的 ReqID，
等待一分钟左右，证书被颁发下来）
Apr 18 10:44:07.007: %PKI-6-CERTRET: Certificate received from Certificate Authority（获取到证书）
fenbu#show crypto ca certificates
（分部获得了根证书和自己的设备证书）
Certificate
Status: Available
Certificate Serial Number: 03
Certificate Usage: General Purpose
Issuer:
cn=zongbu.t31.com
l=changsha
c=CN
Subject:

Name: fenbu.t31.com
hostname=fenbu.t31.com
Validity Date:
start date: 10:43:55 UTC Apr 18 2009
end date: 10:43:55 UTC Apr 18 2010
Associated Trustpoints: 200.1.1.2
CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Issuer:
cn=zongbu.t31.com
l=changsha
c=CN
Subject:
cn=zongbu.t31.com
l=changsha
c=CN
Validity Date:
start date: 10:25:41 UTC Apr 18 2009
end date: 10:25:41 UTC Apr 17 2012
Associated Trustpoints: 200.1.1.2

3.VPN 配置
总部配置:

```
crypto isakmp policy 10
encryption 3des
authentication rsa-sig
hash md5
grou 2
exit
crypto ipsec transform-set tim esp-3des esp-md5-hmac
mode tunnel
exit
crypto map tom 1 ipsec-isakmp
set peer 210.1.1.2
set transform-set tim
match address 101
exit
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
interface ethernet 0/0
crypto map tom
exit
```

分部配置：

```
crypto isakmp policy 10
encryption 3des
authentication rsa-sig
hash md5
grou 2
exit
crypto ipsec transform-set tim esp-3des esp-md5-hmac
mode tunnel
exit
crypto map tom 1 ipsec-isakmp
set peer 200.1.1.2
set transform-set tim
match address 101
exit
access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

interface ethernet 0/0
crypto map tom
exit
```

4. 测试：

```
fenbu#ping 192.168.1.1 source 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 144/145/152 ms
```

5.实验总结：

从本次实验可以得出一个结论，路由器做 ca 服务器又做 VPN 时，
必须自己向自己申请设备证书。

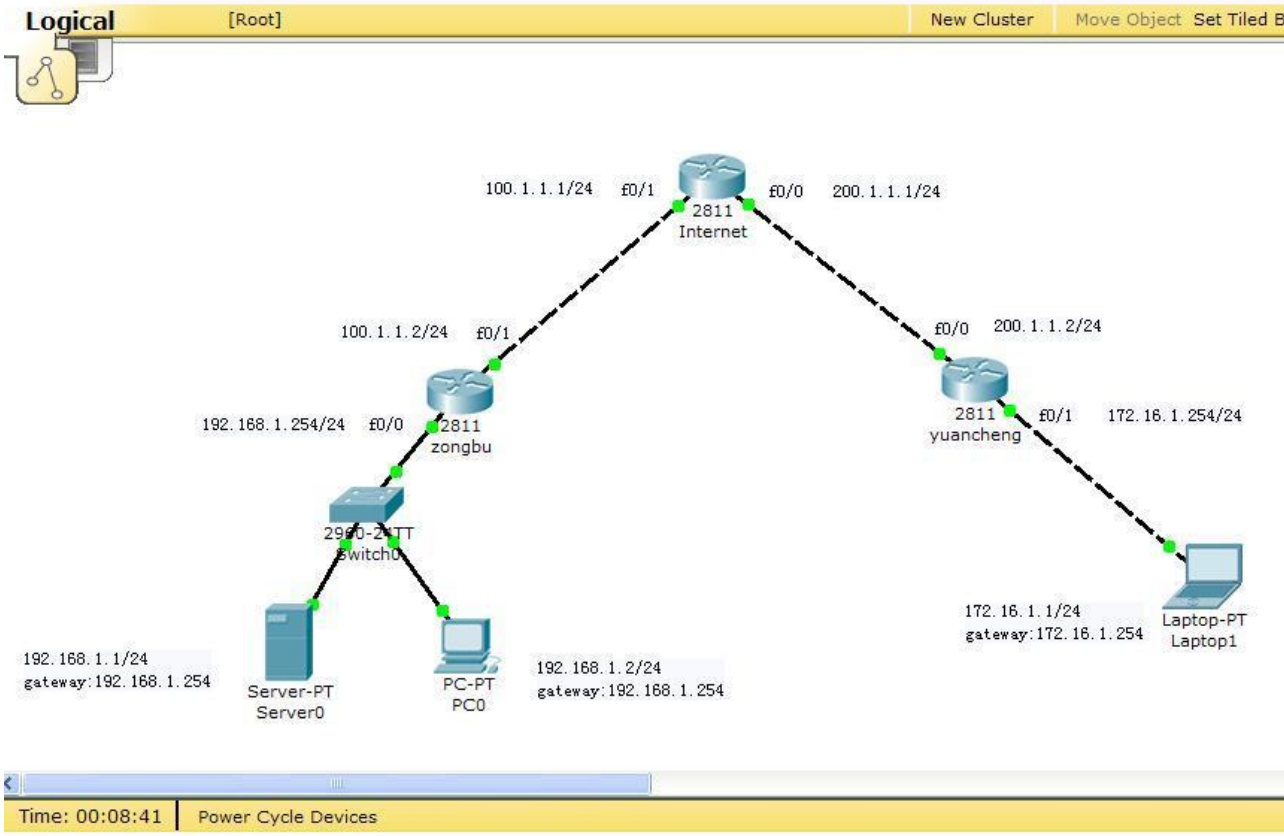
PacketTracer 5.2 基于 AAA 的 Easy VPN 实验

在博客中的《Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南》，所才用接入用户认证是路由器上的用户名密码的本地认证。今天的实验我使用 PacketTracer 5.2（软件下载见我的博客文章《PacketTracer 5.2 的 IPsec VPN 实验说明(附 PacketTracer 5.2 下载地址)》）中自带的 AAA 服务功能来认证授权 Easy VPN。

所谓，AAA 就是认证（Authentication），授权（Authorization），审计（Accounting）这三个英文单词的缩写。（在国内，审计常被称为计费。一切向“钱”看啊！）。简单讲 AAA 的基本工作原理就是，一个事件先必须通过认证才能接入进来；然后根据相应的授权策略，下发相应的权限；审计则记录发生的每件事情。

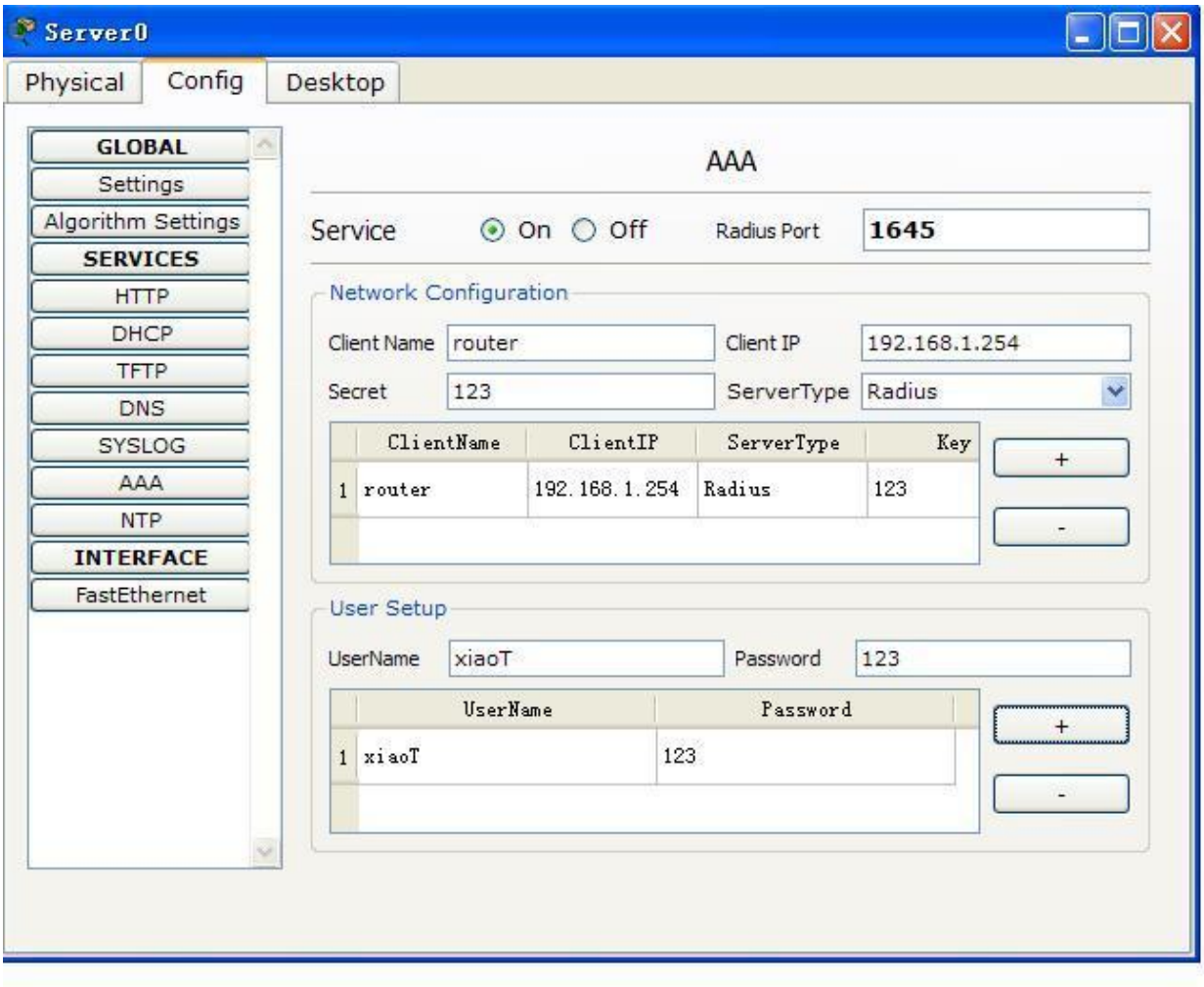
Easy VPN 的讲解见我博客《Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南》。本次就在《Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南》的基础上采用 AAA 服务器，实验的基本连通性配置，也见那篇文章。本次试验重点讲解 AAA。

实验拓扑：



左下角的 AAA 服务器配置如下：

双击服务器图标，选择 Config，在选择 AAA：



AAA 服务器配置简单说明：Clientname 是随意的，Client IP 是你所要管理的路由器或交换机等网络设备的 IP 地址。Secret 是 AAA 服务器与管理的网络设备之间的密钥。ServiceType 是协议内型，Radius 是国际标准，Tacacs 是 cisco 专有协议。本实验使用的 Radius。配置用户名和密码如图所示，点“+”添加。

总部路由的 AAA Easy VPN 配置：

```
aaa new-model
aaa authentication login eza group radius （使用 AAA 认证）
aaa authorization network ezo group radius

radius-server host 192.168.1.1 auth-port 1645 key 123（指点 AAA 服务器的 IP 地址和密钥，1645 是 Radius 的默认端口号）

crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
exit

crypto ipsec transform-set tim esp-3des esp-md5-hmac

ip local pool ez 192.168.3.1 192.168.3.100
crypto isakmp client configuration group myez
 key 123
 pool ez

crypto dynamic-map ezmap 10
 set transform-set tim
 reverse-route
    exit

crypto map tom client authentication list eza
```

```
crypto map tom isakmp authorization list ezo
crypto map tom client configuration address respond
crypto map tom 10 ipsec-isakmp dynamic ezmap

interface fa 0/1
crypto map tom
exit
```

测试：

在远端笔记本的 VPN 中输入如下信息：

GroupName：myez

Group key：123

Host IP(server IP)：100.1.1.2

Username：xiaoT

Password：123

点击 connect，就会提示连接上去，此时会显示下发的 IP 地址。（若没马上连上去，在配置没错的前提下，Ipsec VPN 协商时，前面几个包是不通的，解决方法，在 ping 一下 100.1.1.2，再连接 Easy VPN）。Easy VPN 接入后，就可 ping 总部的任何地址了！

（附件中有基本连通性和最终完成 PKT 文件）。

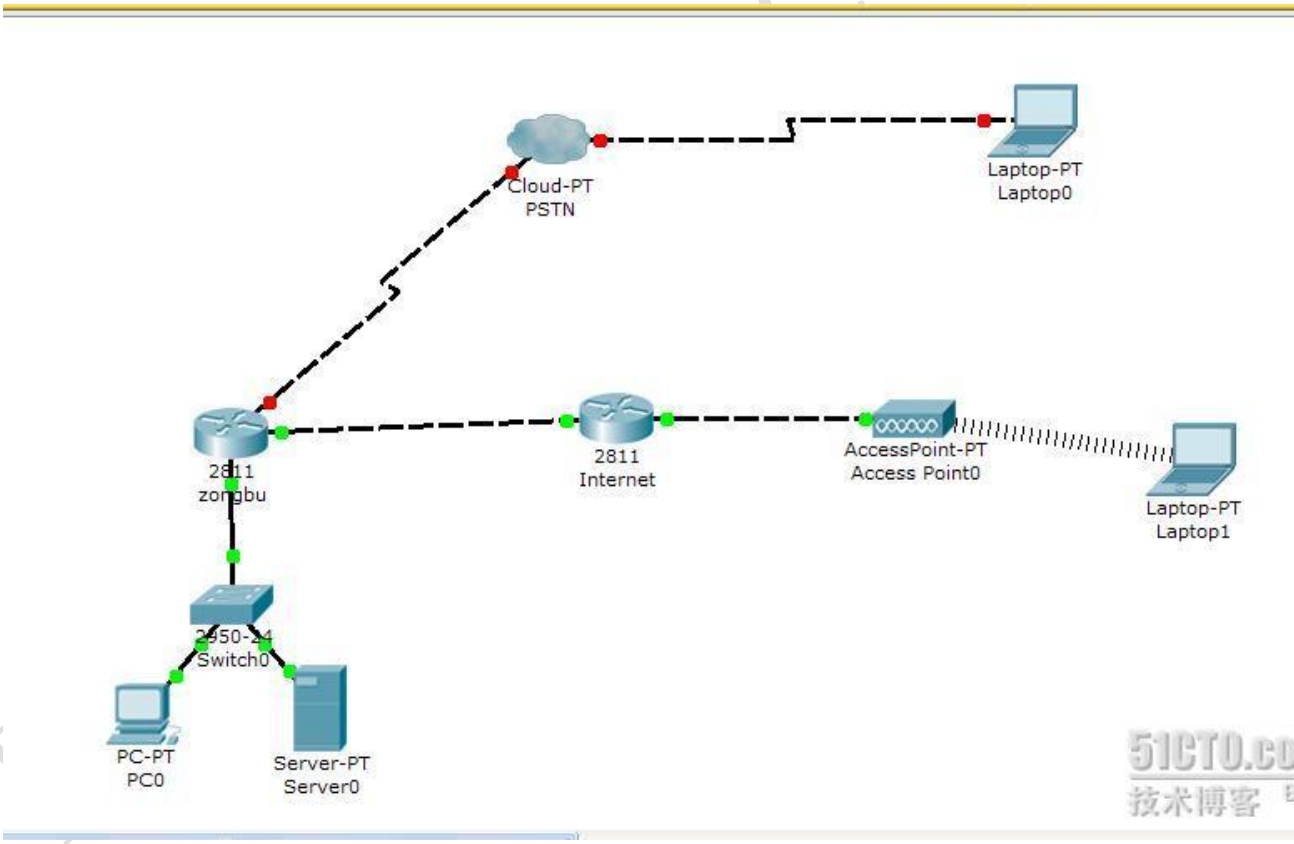
http://9916376.blog.51cto.com/468239/197816

PacketTracer 5.2 之 Easy VPN 与 PSTN 接入实验指南

功夫不负有心人，小 T 我总算弄明白了在 PacketTracer 5.2 上通过做 PSTN（电话网）接入总部的实验了！呵呵。。。废话不多说了，现在就给大家分享下今天的实验。

说实话，在现在的环境中，用 PSTN 接入总部的是已经不常用了，现在常用的是远程 VPN 接入总部，如：Easy VPN ，l2tp，PPTP，SSL VPN 等，远程 VPN 接入的其最大有点就是费用低，只要你所在的地方能上网，那么你就轻松的接入到内容中。但有些情况下，在那些偏远的地方上网时及其不方便的，但一般电话还是用的，这时候，通过 PSTN 网络的接入就起到了作用了！

先讲讲我的今天的网络拓扑思路，请大家先看看我的网络拓扑：



实验思路，一台路由器模拟 Internet 网（就是没有私有 IP 路由表的路由器，本实验没做上网的 NAT，重点强调远程接入），用了一个"网云'来代表 PSTN 网络，总部路由器上换上了电话接口（关于换网络模块见我的博客一文《【交流】浅谈 PacketTracer 5.2 模拟器》中，有详细讲解）。用了一个无线上网来代表所有能上 Internet 网的点。Easy VPN 的实验我就不在这演示了，见我的博

客一文《Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南》。本文重点讲解 PSTN 的接入。

实验的 IP 规划如下：

总部路由器：

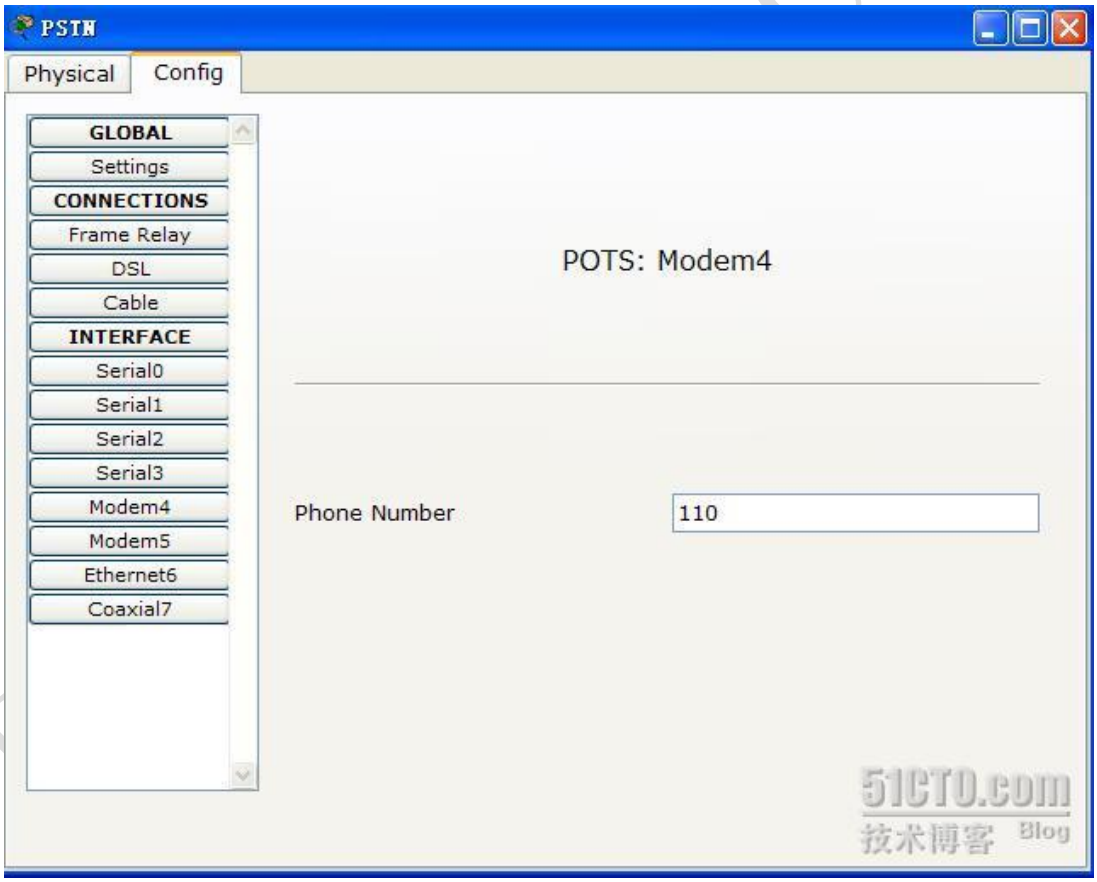
Fa 0/0 192.168.1.254/24 Fa 0/1 100.1.1.2/24

Modem 0/3/0 192.168.3.254/24

Internent 路由器：

Fa 0/1 100.1.1.1/24 Fa 0/1 200.1.1.1/24

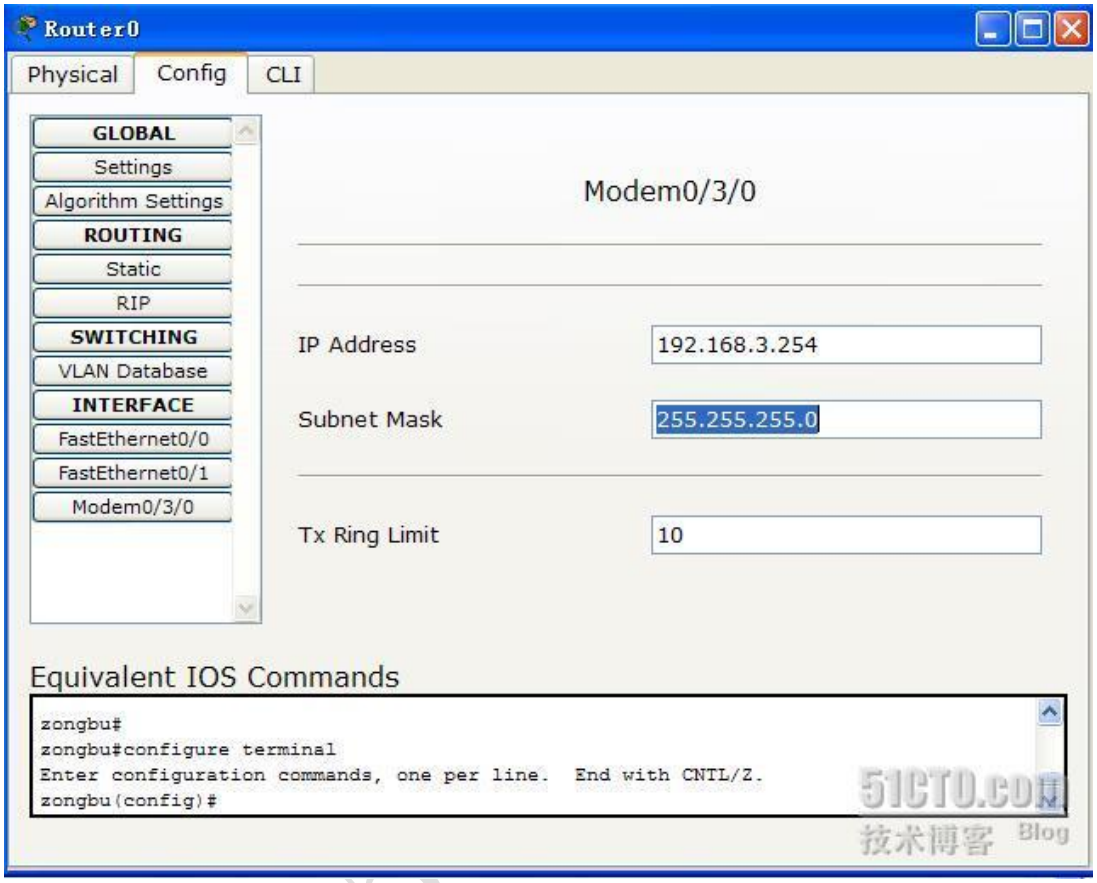
PSTN 网云的配置如下图：



Modem 4 是接总部的 Modem 0/3/0，给总部分配的电话号码是 110，Modem 5 是接远程笔记本的， 给它分配的电话是 120。

实验配置：

总部路由器的的 Modem 0/3/0,（在 config 配置，在 CLI 中配置不了，但最后却在 CLI 中生成了命令，小 T 我弄不明白这是为什么！）配置如图



配置文件：

Internet 网：

```
interface FastEthernet0/0
 ip address 200.1.1.1 255.255.255.0
interface FastEthernet0/1
 ip address 100.1.1.1 255.255.255.0
```

总部路由器：

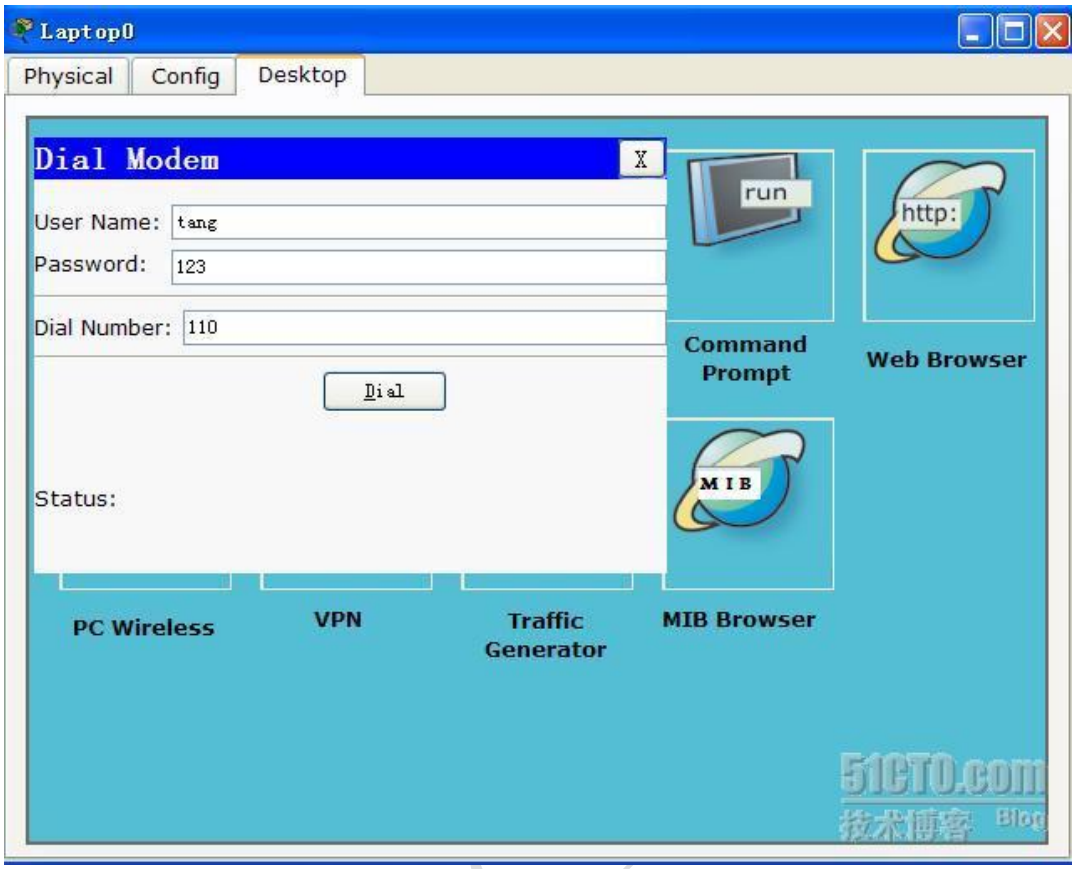
```
hostname zongbu


aaa new-model
```

```
aaa authentication login eza local

aaa authorization network ezo local

username tang password 0 123

crypto isakmp policy 10
 hash md5
 authentication pre-share
 group 2

crypto isakmp client configuration group myez
 key 123
 pool ez


crypto ipsec transform-set tim esp-3des esp-md5-hmac

crypto dynamic-map ezmap 10
 set transform-set tim
 reverse-route

crypto map tom client authentication list eza
crypto map tom isakmp authorization list ezo
crypto map tom client configuration address respond
crypto map tom 10 ipsec-isakmp dynamic ezmap


interface FastEthernet0/0
```

```
 ip address 192.168.1.254 255.255.255.0

interface FastEthernet0/1
 ip address 100.1.1.2 255.255.255.0
 crypto map tom

interface Modem0/3/0
 ip address 192.168.3.254 255.255.255.0
（在路由器，config 中生成的）

ip local pool ez 192.168.2.1 192.168.2.100

ip route 0.0.0.0 0.0.0.0 100.1.1.1

ip dhcp pool PSTN
 network 192.168.3.0 255.255.255.0
 default-router 192.168.3.254
```

测试：

Easy VPN 的接入见我的博客《Cisco PacketTracer 5.2 模拟器的 Easy VPN 实验指南》，讲讲 PSTN 的接入，原理简单的讲，就先拨打通总部的电话 110，然后对用户认证，注意：笔记本网卡设置为 DHCP 获取。在笔记本德 Desktop 中选择 Dial-up，输入信息如图：



点 Dial 就连接上去了，这样就能 ping 通和访问内部服务器。

（附最终完成 PKT 文件）

PacketTracer 5.2 之 GRE 实验（一）

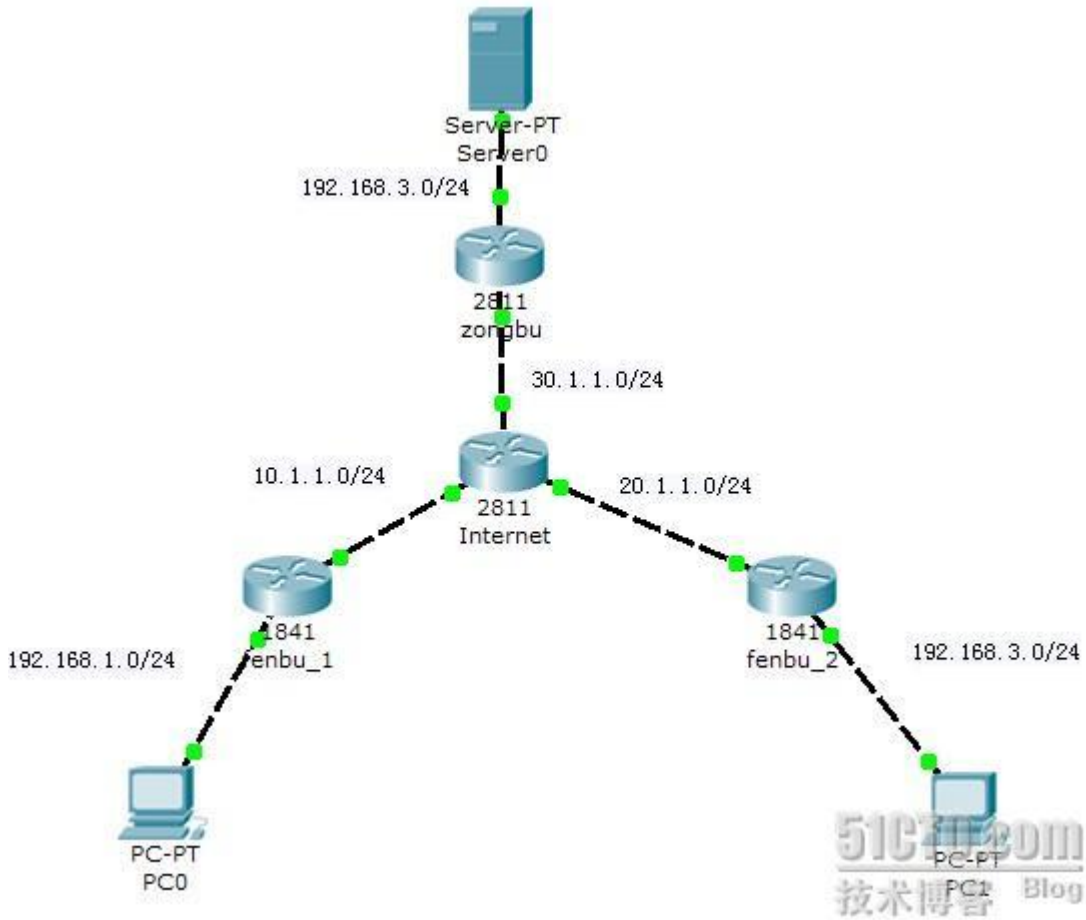
已经快两个月的没写博客。一是年终工作繁琐，二是自己没有合理规划时间，一直没时间写博客，在此对支持和关注的我博客的博友和网友表示歉意。

新年第一篇博文，稍有点紧张。太久没什写博客，在组织言语方面或许比以前有所退步，写不好还请各位批评指正。闲话不多说，开始实验。

GRE：通用路由封装,全称 Generic Routing Encapsulation，也算是 VPN 技术的一种。它能快速、简单地跨越 Internet（公网）实现私网之间连通，特别是在跨越公网组建大的网络。但 GRE 致命的缺点就是，他是明文传输数据。所以在部署 GRE 的时候，往往结合各种安全措施来保护数据，如利用 Ipsec 对其数加密。本文介绍 GRE 的一些简单的实验。

GRE 的原理并不复杂，它只是在私网 IP 包头前再封装一个公网的 IP 包头，而在公网上传输，公网的路由器看的只是公网的 IP 包头的 IP，不会看到私网的 IP 包头，直到到达目标路由器，目标路由器接受到数据后，去除公网 IP 包头发现是 GRE 数据，那么它就将原封不动这个私网 IP 数据传送到内网中（只是 IP 包头以上的数据不动，改变的是二层报头）。我们也可以通俗的理解 GRE，GRE 跟大多数 VPN 一样让整个 Internet 和部署 GRE 的路由器变成了一个路由器，那么两边或多边的网络就像是直接连接在一个路由器上，私网的 IP 就像普通在一个路由器上传输。

首先，看看本次实验的网络拓扑：



IP 规划表：

Internet←→zongbu

Internet 30.1.1.1/24　　zongbu 30.1.1.2/24

Internet←→fenbu_2

Internet 20.1.1.1/24　　fenbu_2 20.1.1.2/24

Internet←→fenbu_1

Internet 10.1.1.1/24　　fenbu_1 10.1.1.2/24

zongbu←→Server

zongbu 192.168.3.254/24　　server 192.168.3.1/24

fenbu_2←→PC1

zongbu 192.168.2.254/24　　PC1　　192.168.2.1/24

fenbu_1←→PC0

zongbu 192.168.2.254/24　　PC0　　192.168.2.1/24

实验说明：

Internet 网还是用一个没有私网 IP 路由器表的路由器代替。基本连通配置见附件的基本连通 PKT 文件。本次验演示静态路由和 GRE，动态路由和 GRE。下面给出 GRE 的关键代码。

静态路由和 GRE：

Zongbu 上路由器配置如下：

interface Tunnel0 （创建 Tunnel 接口 0，此接口在本实验中是与 fenbu_1 建立 GRE）

ip address 1.1.1.1 255.255.255.0 （设置 Tunnel 0 的 IP，此 IP 与 fenbu_1 同一网段）

tunnel source FastEthernet0/0 （GRE 封装时公网源 IP 为 fa 0/0 的 IP）

tunnel destination 10.1.1.2 （GRE 封装是公网目标 IP 为 10.1.1.2 的 IP）

interface Tunnel1 （创建 Tunnel 接口 1，此接口在本实验中是与 fenbu_2 建立 GRE）

ip address 2.1.1.1 255.255.255.0 （设置 Tunnel 1 的 IP，此 IP 与 fenbu_2 同一网段）

tunnel source FastEthernet0/0 （GRE 封装时公网源 IP 为 fa 0/0 的 IP）

tunnel destination 20.1.1.2 （GRE 封装时公网目标 IP 为 20.1.1.2 的 IP）

ip route 192.168.1.0 255.255.255.0 1.1.1.2 （配置通过 GRE 到达 192.168.1.0/24 的静态路由）

ip route 192.168.2.0 255.255.255.0 2.1.1.2 （配置通过 GRE 到达 192.168.2.0/24 的静态路由）

注：fenbu_1、fenbu_2 只列出配置，不再进行说明。

fenbu_1 路由器的配置：

interface Tunnel0

```
 ip address 1.1.1.2 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 30.1.1.2

ip route 192.168.3.0 255.255.255.0 1.1.1.1
ip route 192.168.2.0 255.255.255.0 1.1.1.1
```

fenbu_2 路由器的配置：

```
interface Tunnel0
 ip address 2.1.1.2 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 30.1.1.2
ip route 192.168.3.0 255.255.255.0 2.1.1.1
ip route 192.168.1.0 255.255.255.0 2.1.1.1
```

查看路由表并测试：

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

Gateway of last resort is 30.1.1.1 to network 0.0.0.0

     1.0.0.0/24 is subnetted, 1 subnets
```

```
C       1.1.1.0 is directly connected, Tunnel0
     2.0.0.0/24 is subnetted, 1 subnets
C       2.1.1.0 is directly connected, Tunnel1
     30.0.0.0/24 is subnetted, 1 subnets
C       30.1.1.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 1.1.1.2
S    192.168.2.0/24 [1/0] via 2.1.1.2
C    192.168.3.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 30.1.1.1

fenbu_1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
S    192.168.2.0/24 [1/0] via 1.1.1.1
S    192.168.3.0/24 [1/0] via 1.1.1.1
```

```
S*    0.0.0.0/0 [1/0] via 10.1.1.1


fenbu_2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 20.1.1.1 to network 0.0.0.0

     2.0.0.0/24 is subnetted, 1 subnets
C       2.1.1.0 is directly connected, Tunnel0
     20.0.0.0/24 is subnetted, 1 subnets
C       20.1.1.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 2.1.1.1
C    192.168.2.0/24 is directly connected, FastEthernet0/1
S    192.168.3.0/24 [1/0] via 2.1.1.1
S*   0.0.0.0/0 [1/0] via 20.1.1.1
```

测试方法：总部和各分部ＰＣ相互 ping。

简要数据分析。根据路由表，以 fenbu_1 到总部为例。

Fenbu_1 到 zongbu：

Fenbu_1 中的 PC0(192.168.1.1/24)到 zongbu 的 server(192.168.3.1/24)，PC0 的数据到达 fenbu_1 的路由器，查看路由表到达 192.168.3.0/24 的下一跳 IP 是 1.1.1.1，路由器再次查找路由如何到 1.1.1.1 的，到达 1.1.1.1 是要从 Tu

nnel0 接口出去，此时路由器判断要对数据进行 GRE 封装处理，于是在原有的私有 IP 包报头前封装已经配置好的原公网 IP（fa 0/0 接口 IP）和目标公网 IP（即 zongbu 的 fa 0/0 接口 IP），封装好后，路由器再次查找路由表发现到达 zongbu 的 fa 0/0 从缺省路由出去。就这样数据被送入 Internet（公网），Internet（公网）的路由器直能查看公网 IP 报头，根据公网的目标 IP 转发数据。数据到达 zongbu 后，总部路由器首先看到路由器的目标 IP 是自己的，接受去除公网 IP 报头，发现是一个 GRE 数据，再根据私有 IP 报头中的私有目标 IP 再次查找数据，根据路由表将数据包从 fa 0/1 送至到 server。Server 接受数据，拆封数据查看内容，并产生回应 IP 包到 fenbu_1 的 PC0。此后的过程跟从 PC0 到 server 是一样的 GRE 操作。

未完待续。。。。。。

（附件附有基本连通和完成配置）

http://9916376.blog.51cto.com/468239/268823

PacketTracer 5.2 之 GRE 实验（二）

动态路由和 GRE：（以 OSPF 路由为例）

Zongbu 路由器配置：（命令解释见上一篇）

```
interface Tunnel0
 ip address 1.1.1.1 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 10.1.1.2


interface Tunnel1
 ip address 2.1.1.1 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 20.1.1.2

router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
 network 2.1.1.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
```

fenbu_1 路由器配置：

```
interface Tunnel0
 ip address 1.1.1.2 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 30.1.1.2


router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
```

fenbu_2 路由器配置：

```
interface Tunnel0
 ip address 2.1.1.2 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination 30.1.1.2


router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
 network 2.1.1.0 0.0.0.255 area 0
```

查看 OSPF 邻居表和路由表：

```
zongbu#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.254     0   FULL/  -        00:00:39    1.1.1.2         Tunnel0
192.168.2.254     0   FULL/  -        00:00:38    2.1.1.2         Tunnel1
zongbu#show ip route
Gateway of last resort is 30.1.1.1 to network 0.0.0.0
     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Tunnel0
     2.0.0.0/24 is subnetted, 1 subnets
C       2.1.1.0 is directly connected, Tunnel1
     30.0.0.0/24 is subnetted, 1 subnets
C       30.1.1.0 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/1001] via 1.1.1.2, 00:30:49, Tunnel0
O    192.168.2.0/24 [110/1001] via 2.1.1.2, 00:30:49, Tunnel1
C    192.168.3.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 30.1.1.1
```

```
fenbu_1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.3.254     0   FULL/  -        00:00:36    1.1.1.1         Tunnel0
fenbu_1#show ip route
Gateway of last resort is 10.1.1.1 to network 0.0.0.0
     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Tunnel0
     2.0.0.0/24 is subnetted, 1 subnets
O       2.1.1.0 [110/2000] via 1.1.1.1, 00:28:13, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
O    192.168.2.0/24 [110/2001] via 1.1.1.1, 00:28:03, Tunnel0
O    192.168.3.0/24 [110/1001] via 1.1.1.1, 00:28:13, Tunnel0
S*   0.0.0.0/0 [1/0] via 10.1.1.1
```

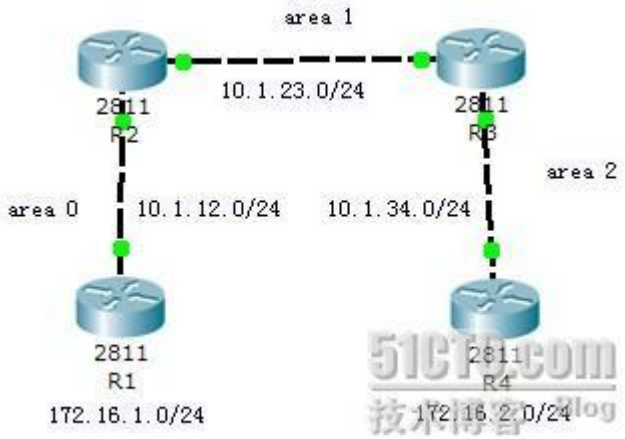
```
fenbu_2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
```

```
192.168.3.254      0   FULL/  -        00:00:38    2.1.1.1         Tunnel0
fenbu_2#show ip route
Gateway of last resort is 20.1.1.1 to network 0.0.0.0
     1.0.0.0/24 is subnetted, 1 subnets
O       1.1.1.0 [110/2000] via 2.1.1.1, 00:26:12, Tunnel0
     2.0.0.0/24 is subnetted, 1 subnets
C       2.1.1.0 is directly connected, Tunnel0
     20.0.0.0/24 is subnetted, 1 subnets
C       20.1.1.0 is directly connected, FastEthernet0/0
O    192.168.1.0/24 [110/2001] via 2.1.1.1, 00:26:02, Tunnel0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
O    192.168.3.0/24 [110/1001] via 2.1.1.1, 00:26:12, Tunnel0
S*   0.0.0.0/0 [1/0] via 20.1.1.1
```

简要分析：从上面的 ospf 邻居表和路由表来看，所形成的路由跟用普通的几个路由器配置 ospf 结果大致是一样的。那么 ospf 的路由信息是怎样通过 GRE 传递过去的呢？首先，路由器发起带有本地路由器信息的协议数据包，数据从从 Tunnel 接口发布出去（ospf 的配置中发布这个接口的 IP），路由器发现要对数据进行 GRE 处理，于是就给这个数据包加上公网目标和原 IP，然后数据就在公网中传递到目标路由器，目标路由器接受并拆封数据，发现是 GRE 数据，再拆分和查看私网 IP 数据，学习到了 OSPF 的路由信息，后面的过程就跟 OSPF 路由协议的原理是一样的，只不过是在公网传输经过了 GRE 处理。

GRE 代替 OSPF 的虚链路，完成跨普通区域与主干区域连接。其原理还是一样的，在原有的 IP 上再封装一层 IP 报头（这 IP 报头是在所需要跨域的区域中，是有路由的。你也可以把这些区域想象成公网）。

拓扑图如下：



详细的 IP 配置见附件，下面只显示下 GRE 关键配置。

R2 路由器：

```
interface Tunnel0
 ip address 1.1.1.2 255.255.255.0
 tunnel source FastEthernet0/1
 tunnel destination 10.1.23.1

router ospf 1
 network 10.1.12.0 0.0.0.255 area 0
 network 1.1.1.0 0.0.0.255 area 0
 network 10.1.23.0 0.0.0.255 area 1
```

R3 路由器：

```
interface Tunnel0
 ip address 1.1.1.1 255.255.255.0
 tunnel source FastEthernet0/1
 tunnel destination 10.1.23.2

router ospf 1
 log-adjacency-changes
```

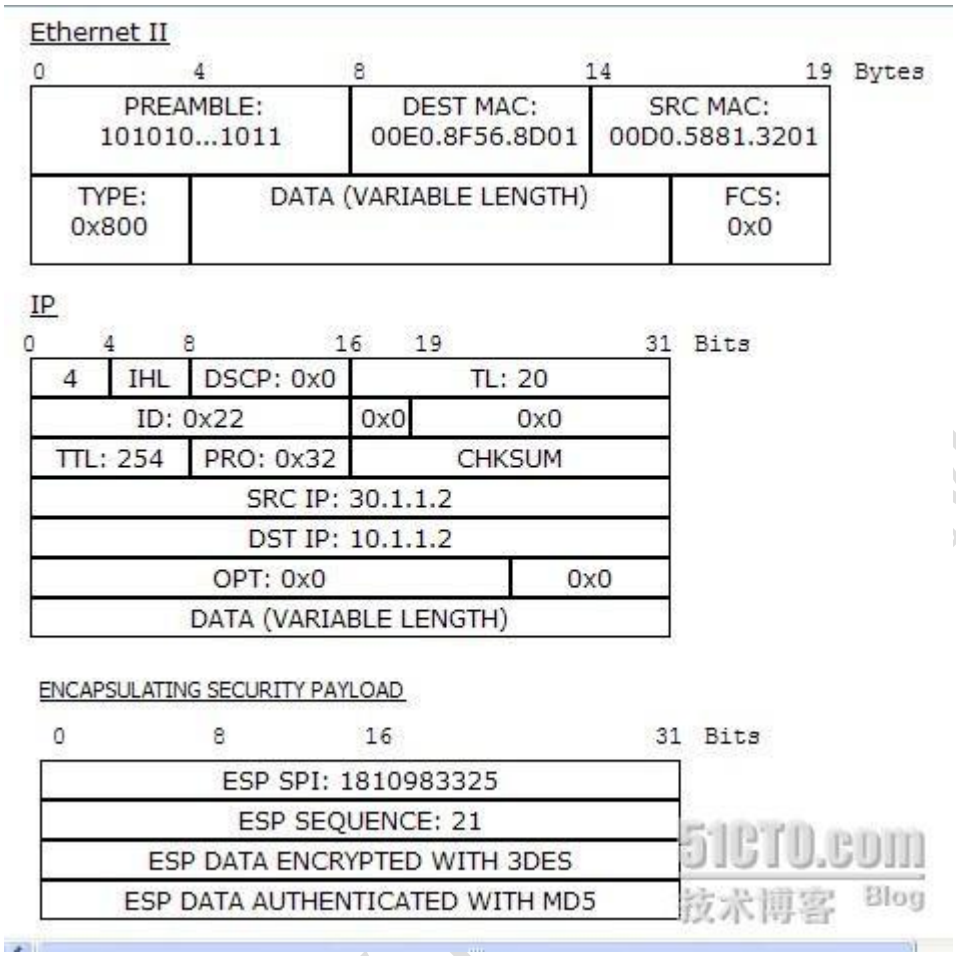
```
network 10.1.34.0 0.0.0.255 area 2
network 10.1.23.0 0.0.0.255 area 1
network 1.1.1.0 0.0.0.255 area 0
```

查看路由表，和 OSPF 邻居表，请各位下载附件，仔细观察，我就不重复了。

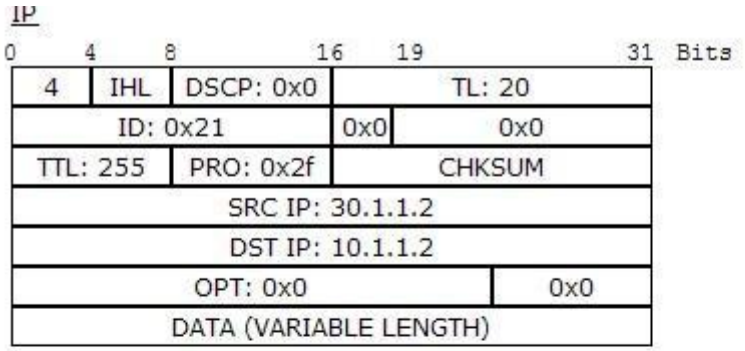
PacketTracer 5.2 之 GRE 实验(三)

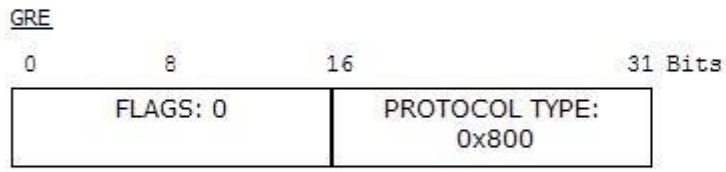
GRE 的方便迅速跨域公网实现内部私网的通信，但 GRE 有着一个致命的缺点：明文传输数据。在公网这个极其不安全的网络上，明文传输数据时很危险，特别是办公的涉密数据。所以，为保护数据 GRE 数据我们可以结合 Ipsec VPN 的技术来提供对 GRE 的加密，提高安全性。（或许大家回想，用 Ipsec VPN 就可以，怎么还用 GRE？呵呵。。。我个人觉得在学习的时候，各种技术学了之后，才能深刻的体会各种技术的有点和缺点，在实际工作，我们就可以选择适合的技术来实施）。

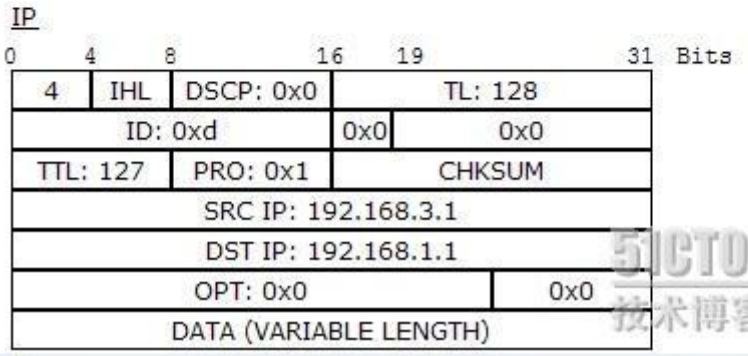
GRE 和 Ipsec VPN 的结合使用，大致可分为：GRE Over Ipsec 和 Ipsec Over GRE。GRE Over Ipsec，顾名思义就是整个 GRE 数据被 Ipsec VPN 加密所承载。Ipsec Over GRE，则是 Ipsec VPN 的数据被 GRE 所承载，先用 GRE 快速连通网络，再利用 Ipsec VPN 对关键数据进行加密后再被 GRE 所承载，非关键数据还是明文传输的 GRE。（本文以 GRE Over Ipsec 为例）下面是 GRE Over Ipsec 传输数据，用 PT 5.2 抓的数据包结构图：

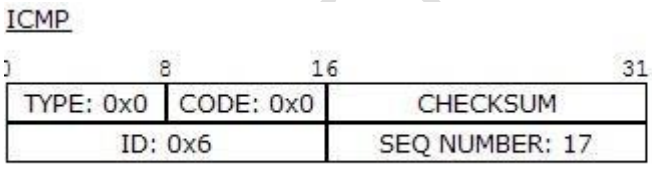


这个是在公网那个上看到的包结构，最下面是 Ipsec 报文头部，后面的数据时看不到的，但 PT 作为一款不错的初级入门学习模拟器，在包的结构显示上较为清楚。









上图就是 Ipsec VPN 封装内部的结构。

现在以 GRE Over Ipsec 为例演示实验。

基本配置（见 http://9916376.blog.51cto.com/468239/268823，在此基础上部署 Ipsec VPN）。

关键配置如下：（以总部路由器为例，详细的配置见附件 PKT 文件中查看，Ipsec VPN 配置命令的解释，大家查阅资料，比我写的好多了）

Zongbu 路由器：

```
crypto isakmp policy 10
```

```
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp key xiaot1 address 10.1.1.2
crypto isakmp key xiaot2 address 20.1.1.2

crypto ipsec transform-set tim esp-3des esp-md5-hmac

access-list 101 permit ip host 30.1.1.2 host 10.1.1.2
access-list 102 permit ip host 30.1.1.2 host 20.1.1.2

crypto map tom 10 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set tim
 match address 101

crypto map tom 20 ipsec-isakmp
 set peer 20.1.1.2
 set transform-set tim
 match address 102

interface FastEthernet0/0
crypto map tom
```

GRE Over Ipsec 在配置 Ipsec 策略的时候，重点是分析我们所需要保护的流量，即要保护的源 IP 和目标 IP 是什么。在数据到达 fa 0/0 接口之前，私网

数据被 GRE 处理打上了公网的 IP 数据，数据送至 fa 0/0 接口，发现是公网的源 IP 和目标 IP，由于 fa 0/0 绑定了 Ipsec VPN 策略，只有符合要求的数量才会触发 Ipsec，才能被 Ipsec 所保护，故在上面的配置（见红色配置），ACL 定义感兴趣流量就是公网的源 IP 和目标，而非我们普通 Ipsec VPN 配置写的是私网的源 IP 和目标 IP。

测试，简单说明下，PC Ping Server 要多 ping 几次，Ipsec VPN 的协商丢包现象是正常，耐心等待。

Ipsec Over GRE 简单说明，因为 GRE 先解决了私网连通性了，故针对关键数据 Ipsec 保护，配置 Ipsec 策略的时候，就是具体的私网的源 IP 和目标 IP。

附件：http://9916376.blog.51cto.com/468239/272035