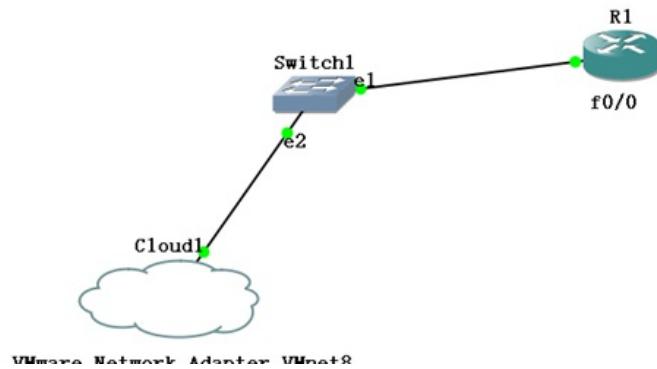


# 实验一、PPPoE实验

## 一、实验目的

- 1、掌握 PPPoE 服务器搭建和配置的方法
- 2、掌握客户端创建 PPPoE 拨号连接的方法
- 3、分析 PPPoE 协议工作过程
- 4、理解 PPPoE 的两种认证方法。

## 二、实验拓扑



## 三、实验步骤

- 1、根据实验拓扑搭建利用 GNS3 搭建实验环境，注意，路由器型号用 7200。
- 2、配置路由器 R1，将其配置为 PPPoE 服务器，参考命令如下（注：下面 IP 地址的第 2 字节修改为自己班级，第 3 字节修改为自己学号后两位）。

```
R1(config)#hostname PPPoE 路由器名称修改为自己姓名拼音  
PPPoE(config)#interface lo0 配置回环接口用于模拟 Internet  
PPPoE(config-if)#ip address 211.1.29.16 255.255.255.0  
PPPoE(config-if)#ip address 8.1.29.8 255.255.255.0 secondary  
PPPoE(config-if)#no shutdown
```

配置 DHCP 服务器，并命名为 smy，此处修改为自己的姓名拼音

```
PPPoE(config)#ip dhcp pool smy  
PPPoE(dhcp config)#network 192.1.29.0 /24          配置地址池  
PPPoE(dhcp config)#dns-server 211.1.29.16 8.1.29.8  配置 DNS 服务器地址  
PPPoE(dhcp config)#default-router 192.1.29.254      配置默认网关
```

添加排除 IP 地址 192.1.29.1，因为此地址要分配给虚拟模板使用，注意要在全局配置模式下配置

```
PPPoE(config)#ip dhcp excluded-address 192.1.29.1    配置虚拟模板用于实施对于客户端的身份验证，使用 PAP 认证。  
PPPoE(config)#interface virtual-template 129        模板编号修改为自己学号后 3 位  
PPPoE(config-if)#encapsulation ppp  
PPPoE(config-if)#ppp authentication pap  
PPPoE(config-if)#peer default ip address dhcp-pool smy  
PPPoE(config-if)#ip address 192.1.29.1 255.255.255.0  
PPPoE(config-if)#no shutdown
```

启用 VPDN，并配置 VPDN 的组 1，指出接受客户端呼叫。并且采用 PPPOE 的协议。同时使用虚拟模板 1 的参数与客户端协商。

```
PPPoE(config)#vpdn enable  
PPPoE(config)#vpdn-group 129  
PPPoE(config-vpdn)#accept-dialin           vpdn 组编号修改为自己学号后 3 位
```

接受客户端呼叫

```
PPPoE(config-vpdn-acc-in)#protocol pppoe  
PPPoE(config-vpdn-acc-in)#virtual-template 129      模板编号修改为自己学号后 3 位
```

在接口 f0/0 上启用 PPPoE

```
PPPoE(config)#interface f0/0  
PPPoE(config-if)#pppoe enable  
PPPoE(config-if)#no shutdown
```

创建本地登录用户名和密码，用户名修改为自己的姓名，密码修改为自己的学号。

```
PPPoE(config)#username smy password 129
```

问题 1：在本地查看路由表，能看到哪些选项？（截图）

```
smy#show ip route  
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
      E1 - OSPF external type 1, E2 - OSPF external type 2  
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
      ia - IS-IS inter area, * - candidate default, U - per-user static route  
      o - ODR, P - periodic downloaded static route  
  
Gateway of last resort is not set  
  
C    211.1.29.0/24 is directly connected, Loopback0  
      8.0.0.0/24 is subnetted, 1 subnets
```

问题 2：在特权模式下输入命令 show running-config | section dhcp 查看到的结果

```
smy#show running-config | section dhcp  
ip dhcp excluded-address 192.1.29.1  
ip dhcp pool smy  
  network 192.1.29.0 255.255.255.0  
  dns-server 211.1.29.16 8.1.29.8  
  default-router 192.1.29.254
```

问题 3：在特权模式下输入命令 show running-config | section Template 查看到的结果

```
smy# show running-config | section Template  
interface Virtual-Template129  
  ip address 192.1.29.1 255.255.255.0
```

3、在主机上创建连接拨号。

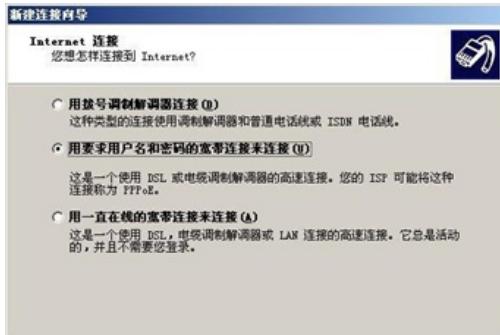
单击【开始】—【程序】—【附件】—【通讯】—【新建连接向导】，打开新建连接向导。



单击【下一步】，选择“连接到 Internet”



单击【下一步】，选择“要求用户名和密码的宽带连接来连接”选项



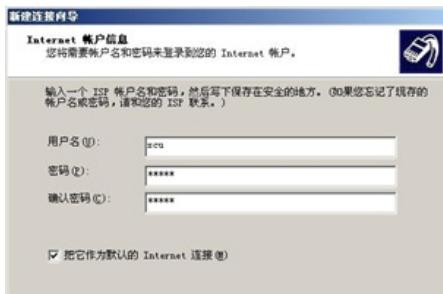
单击【下一步】，输入宽带连接的名称



单击【下一步】，选择“只允许我使用”选项



单击【下一步】，输入用户名和密码，改用户名和密码为在路由器上配置的用户名和密码，即自己的姓名和学号



单击【下一步】，把“在桌面上添加快捷方式”复选框选中，单击【完成】按钮，完成新建连接向导。



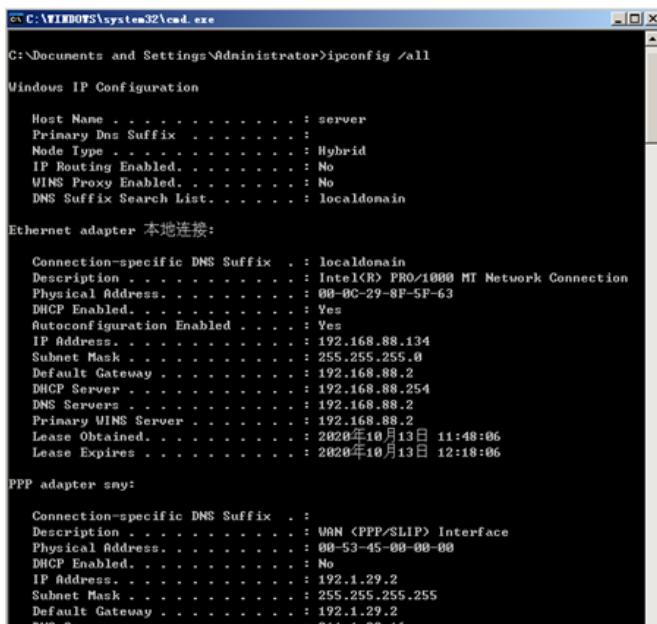
如图看到smy建立成功

4、打开抓包工具 Wireshark 或者 Sniffer，开启抓取数据包，单击桌面上的新建连接，单击连接按钮

问题 4：此时能否连接上？在主机中打开命令行，用 ipconfig /all 查看本地连接情况



如图所示，能连接上，查看IP地址



看到本地连接IP地址为192.168.88.134

看到最后有PPP连接，IP地址为192.1.29.2

子网掩码为255.255.255.255, 网关为192.1.29.2

DNS1为211.1.29.16，DNS2为8.1.29.8

问题 5：在主机中 ping 211.1.29.16 和 64.100.58.33。查看能否 ping 通

```
C:\Documents and Settings\Administrator>ping 211.1.29.16
Pinging 211.1.29.16 with 32 bytes of data:
Reply from 211.1.29.16: bytes=32 time=22ms TTL=255
Reply from 211.1.29.16: bytes=32 time=15ms TTL=255
Reply from 211.1.29.16: bytes=32 time=15ms TTL=255
Reply from 211.1.29.16: bytes=32 time=15ms TTL=255

Ping statistics for 211.1.29.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
C:\Documents and Settings\Administrator>ping 64.100.58.33
Pinging 64.100.58.33 with 32 bytes of data:
Reply from 192.1.29.1: Destination host unreachable.

Ping statistics for 64.100.58.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

问题 6：在路由器上输入 show pppoe session，查看结果

```
PPPoE#show pppoe session
 1 session in LOCALLY_TERMINATED (PTA) State
 1 session total

Uniq ID      PPPoE      RemMAC          Port          Source      VA          State
          SID      LocMAC
```

问题 7：在路由器上输入 show ip dhcp binding，查看结果

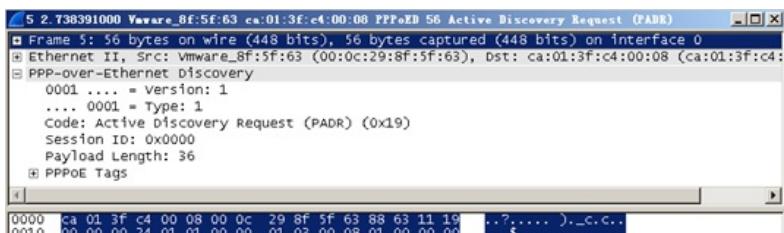
```
PPPoE#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/           Lease expiration      Type
                  Hardware address/
```

5、断开连接，然后停止数据抓包，把抓取的数据报保存下来，文件名“班级\_姓名\_学号”。

6、打开抓取的数据报，查看抓取的报文中 PPPoE 发现阶段使用了几个报文？PPPoE 报文的版本号和 Type 类型是多少？

发现阶段使用了四个报文：PADI、PADO、PADR、PADS

```
3 2.72992900 VMware_8f:5f:63      Broadcast      PPPoE      36 Active discovery Initiation (PADI)
4 2.73834100 ca:01:3f:c4:00:08 VMware_8f:5f:63      PPPoE      45 Active discovery Offer (PADO) 'SessionID:0x0000'
```



PPPoE 报文的版本号为 1

Type 类型为 1

Version: 1

Type: 1

7、根据抓取的数据包填写下表

表 1-1 PPPoE 发现阶段报文

| 数据链路层                 |                           |                                | PPPoE 层   |            |    |                          |         |
|-----------------------|---------------------------|--------------------------------|---|------------|----|--------------------------|---------|
| 目的 MAC                | 源 MAC                     | 链路层 Type                       | Code  | Session ID | 长度 | Uniq                     | Cookie  |
| ff:ff:ff:f<br>f:ff:ff | 00:0c:2<br>9:8f:5f:<br>63 | PPPoE<br>Discovery<br>(0x8863) | Active<br>Discovery<br>Initiation(PADI)<br>(0x09) | 0x0000     | 16 | 010000<br>000100<br>0000 |         |
| 00:0c:2               | ca:01:3                   | PPPoE                          | Active  | 0x0000     | 45 | 010000                   | 8e07a5a |

|                           |                           |                                |   |        |    |                          |  |
|---------------------------|---------------------------|--------------------------------|---|--------|----|--------------------------|--|
| 9:8f:5f:<br>63            | f:c4:00:<br>08            | Discovery<br>(0x8863)          | Discovery<br>Offer(PADO)(0<br>x07)                  |        |    | 000100<br>0000           | 192841f<br>3ee357ca<br>9c0ae2d<br>deb            |
| ca:01:3f<br>:c4:00:0<br>8 | 00:0c:2<br>9:8f:5f:<br>63 | PPPoE<br>Discovery<br>(0x8863) | Active<br>Discovery<br>Request(PADR)<br>(0x19)      | 0x0000 | 36 | 010000<br>000200<br>0000 | 8e07a5a<br>192841f<br>3ee357ca<br>9c0ae2d<br>deb |
| 00:0c:2<br>9:8f:5f:<br>63 | ca:01:3<br>f:c4:00:<br>08 | PPPoE<br>Discovery<br>(0x8863) | Active<br>Discovery<br>Session-<br>confirmation(PA) | 0x0001 | 36 | 010000<br>000200<br>0000 | 8e07a5a<br>192841f<br>3ee357ca<br>9c0ae2d        |

报文编号 2 1. 97958900 ca:01:3f:c4:00:08 CDP/VT/PTP/PAgP/UD/CDP 357 Device ID: PPPoE Port ID: FastEthernet0/0  
 报文内容 992900 VMware\_8f:5f:63 Broadcast PPPoED 36 Active Discovery Initiation (PADI)  
 Frame 3: 36 bytes on wire (288 bits), 36 bytes captured (288 bits) on Interface 0  
 Ethernet II, Src: VMware\_8f:5f:63 (00:0c:29:8f:5f:63), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Destination: Broadcast (ff:ff:ff:ff:ff:ff) 目的MAC地址  
 Address: Broadcast (ff:ff:ff:ff:ff:ff)  
 .... ..1 ..... .... = LG bit: Locally administered address (this is NOT the factory default)  
 .... ..1 ..... .... = TG bit: Group address (multicast/broadcast)  
 Source: VMware\_8f:5f:63 (00:0c:29:8f:5f:63) 源MAC地址  
 Address: VMware\_8f:5f:63 (00:0c:29:8f:5f:63)  
 .... ..0 ..... .... = LG bit: Globally unique address (factory default)  
 .... ..0 ..... .... = IG bit: Individual address (unicast)  
 Type: PPPoE Discovery (0x8863) 链路层类型  
 PPP-over-Ethernet Discovery  
 0001 .... = Version: 1 版本号为1  
 .... 0001 = Type: 1  
 Code: Active Discovery Initiation (PADI) (0x09)  
 Session ID: 0x0000  
 Payload length: 14 长度

8、在抓取的数据包中查找 LCP 报文，查看在 LCP 配置阶段最后一个 LCP 报文的编号是多少？Option 选项有哪些，这些选项的值是多少？（提示，查找最后协商结果报文）

编号为40

Option 选项有Identifier、Length、Magic Number、Data

Identifier: 3 (0x03)

Length: 12

Magic Number: 0x58aa5cf7

Data: 58aa5cf7

Frame 40: 34 bytes on wire (272 bits), 34 bytes captured (272 bits) on Interface 0  
 Ethernet II, Src: VMware\_8f:5f:63 (00:0c:29:8f:5f:63), Dst: ca:01:3f:c4:00:08 (ca:01:3f:c4:00:08)  
 Destination: ca:01:3f:c4:00:08 (ca:01:3f:c4:00:08)  
 Address: ca:01:3f:c4:00:08 (ca:01:3f:c4:00:08)  
 .... ..1 ..... .... = LG bit: Locally administered address (this is NOT the factory default)  
 .... ..0 ..... .... = IG bit: Individual address (unicast)  
 Source: VMware\_8f:5f:63 (00:0c:29:8f:5f:63)  
 Address: VMware\_8f:5f:63 (00:0c:29:8f:5f:63)  
 .... ..0 ..... .... = LG bit: Globally unique address (factory default)  
 .... ..0 ..... .... = IG bit: Individual address (unicast)  
 Type: PPPoE Session (0x8864)  
 PPP-over-Ethernet Session  
 0001 .... = version: 1  
 .... 0001 = Type: 1  
 Code: Session Data (0x00)  
 Session ID: 0x0001  
 Payload Length: 14  
 Point-to-Point Protocol  
 Protocol: Link Control Protocol (0xc021)  
 PPP Link Control Protocol  
 Code: Echo Reply (10)  
 Identifier: 3 (0x03)  
 Length: 12  
 Magic Number: 0x58aa5cf7  
 Data: 58aa5cf7

9、查看 PAP 认证报文，填写表 1-2，没有的话空着。

表 1-2 PAP 认证

|          | 报文编号 | PPP 协议类型                               | Code                        | ID     | 长度 | 用户名 | 密码  |
|----------|------|--|-----------------------------|--------|----|-----|-----|
| 认证<br>请求 | 19   | Authentication<br>Protocol<br>(0xc023) | Authenticate-<br>Request(1) | 0x0001 | 12 | smy | 129 |
| 认证<br>响应 | 20   | Authentication<br>Protocol             | Authenticate-<br>ACK(2)     | 0x0001 | 5  |     |     |

10、在抓取的报文中找到分配 IP 地址的报文编号，使用什么协议分配的，分配 DNS 服务器地址的报文编号是什么？是使用什么协议分配的？

在抓取的报文中找到分配 IP 地址的报文编号，使用PPP IPCP协议分配的。

|                                 |                   |          |                          |
|---------------------------------|-------------------|----------|--------------------------|
| 24 4.41735800 ca:01:3f:c4:00:08 | Vmware_8f:5f:63   | PPP LCP  | 60 Echo Request          |
| 25 4.42709700 Vmware_8f:5f:63   | ca:01:3f:c4:00:08 | PPP LCP  | 34 Echo Reply            |
| 26 5.08765900 Vmware_8f:5f:63   | ca:01:3f:c4:00:08 | PPP IPCP | 56 Configuration Request |
| 27 5.42774800 ca:01:3f:c4:00:08 | Vmware_8f:5f:63   | PPP IPCP | 60 Configuration Request |
| 28 5.44696200 Vmware_8f:5f:63   | ca:01:3f:c4:00:08 | PPP IPCP | 32 Configuration Ack     |

分配 DNS 服务器地址的报文编号是35、36，是使用DHCP协议分配的。

|                                 |                 |          |   |
|---------------------------------|-----------------|----------|---|
| 34 5.54727800 ca:01:3f:c4:00:08 | Vmware_8f:5f:63 | PPP IPCP | 60 Configuration Ack                        |
| 35 5.55566001 00:0c:29:8f:63:02 | 255.255.255.255 | DHCP     | 350 DHCP Inform - Transaction ID: 0xcfa340f |

11、在路由器上修改认证方式为 chap，配置命令如下：

```
PPPoE(config)#interface virtual-template 1 模板编号修改为自己学号后 3 位
PPPoE(config-if)#ppp authentication mschap-v2
```

12、配置后，打开 Wireshark 抓包，重新连接，查看能否连接上，如果能的话断开连接，停止抓包，把抓取的数据包文件命名为“班级\_姓名\_学号 2”。

能连接上

13、打开抓取的数据报，查找到 CHAP 认证的报文，根据报文填写表 1-3，没有的字段空着 value 值填前 3 个字节的十六进制值，Message 填前 6 个字符

|                                  |                   |          |  |
|----------------------------------|-------------------|----------|--|
| 329 442.449211 ca:01:3f:c4:00:08 | Vmware_8f:5f:63   | PPP LCP  | 60 Challenge_Chain=PPPOE , VALUE=0x53fa37807d11755825eda278fde830)                   |
| 331 442.449644 Vmware_8f:5f:63   | ca:01:3f:c4:00:08 | PPP LCP  | 40 Identification  |
| 331 442.449723 Vmware_8f:5f:63   | ca:01:3f:c4:00:08 | PPP LCP  | 44 Identification  |
| 332 442.593195 Vmware_8f:5f:63   | ca:01:3f:c4:00:08 | PPP CHAP | 79 Response (NAME='smy' , VALUE=0xf712978d9f224c78669ef95b357443a0000000000000000..) |
| 333 442.860811 ca:01:3f:c4:00:08 | Vmware_8f:5f:63   | PPP CHAP | 68 Success (MESSAGE= S=65DC9C11C74A3BE51D5AB1C410CA201009685F )                      |

Frame 329: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
Ethernet II, Src: Vmware\_8f:5f:63 (00:0c:29:8f:63:00), Dst: Vmware\_8f:5f:63 (00:0c:29:8f:63:00)  
**destination: Vmware\_8f:5f:63 (00:0c:29:8f:63:00)**  
Address: Vmware\_8f:5f:63 (00:0c:29:8f:5f:63)  
...0..... = LG bit: Globally unique address (factory default)  
...0..... = IG bit: Individual address (unicast)  
**Source: ca:01:3f:c4:00:08 (ca:01:3f:c4:00:08)**  
Address: ca:01:3f:c4:00:08 (ca:01:3f:c4:00:08)  
...1..... = LG bit: Locally administered address (this is NOT the factory default)  
...0..... = IG bit: Individual address (unicast)  
Type: PPPoE Session (0x8B64)  
PPPoE Session Information  
0001 ... = version 1  
... 0001 = Type: 1  
code: session data (0x00)  
Session ID: 0x0000  
Duration: 1 second

表 1-3 CHAP 认证

| 报文编号 | PPP 协议  | Code         | ID | 长度 | Value size | Value                                     | Name | Message   |
|------|---|--------------|----|----|------------|---|------|-----------|
| 329  | Challenge Handshake Authentication Protocol(0xc223) | Challenge(1) | 1  | 28 | 16         | 553fa378676c11755825eda278fde830          | smy  |           |
| 332  | Challenge Handshake Authentication Protocol(0xc223) | Response(2)  | 1  | 57 | 49         | f712978d9f224c78669ef95b357443a00000000.. | smy  |           |
| 333  | Challenge Handshake Authentication Protocol(0xc223) | Success(3)   | 1  | 46 |            |   |      | S=65DC C9 |

14、根据实验，自己描述 PPPoE 从开始连接到释放连接的过程，要详细。

PPPoE的工作过程分成两个阶段，即发现阶段(Discovery)和PPP会话阶段。

(1) 发现阶段(Discovery Stage)的具体过程如下:

- 1 用户主机用广播的方式发出PADI (PPPOE Active Discovery Initiation) 包, 准备去获得所有可连接的接入设备 (获得其MAC地址) ;
- 2 接入设备收到PADI包后, 返回PADO (PPPOE Active Discovery Offer) 作为回应;
- 3 用户主机从收到的多个PADO包中, 根据其名称类型名或者服务名, 选择一个合适的接入设备, 然后发送PADR (PPPOE Active Discovery Request) 包, 另外如果一个用户主机在发出PADI后在规定时间内没有收到PADO, 则会重发PADI;
- 4 接入设备收到PADR包后, 返回PAS (PPPOE Active Discovery Session-confirmation) 包, 其中包含了一个唯一session ID, 双方进入PPP会话阶段。

(2) PPP会话阶段, 即在session建立后的通讯阶段。

无论是用户主机还是接入设备可随时发起PADT包, 中止通讯, 释放连接。