



认证培训

1) 差异化管理

2) 计费

3) 实名审计

■BAS/BRAS

宽带接入服务器 (Broadband Access Server/ Broadband Remote Access Server)

■AAA

AAA是验证、授权和记账 (Authentication、Authorization、Accounting) 三个英文单词的简称

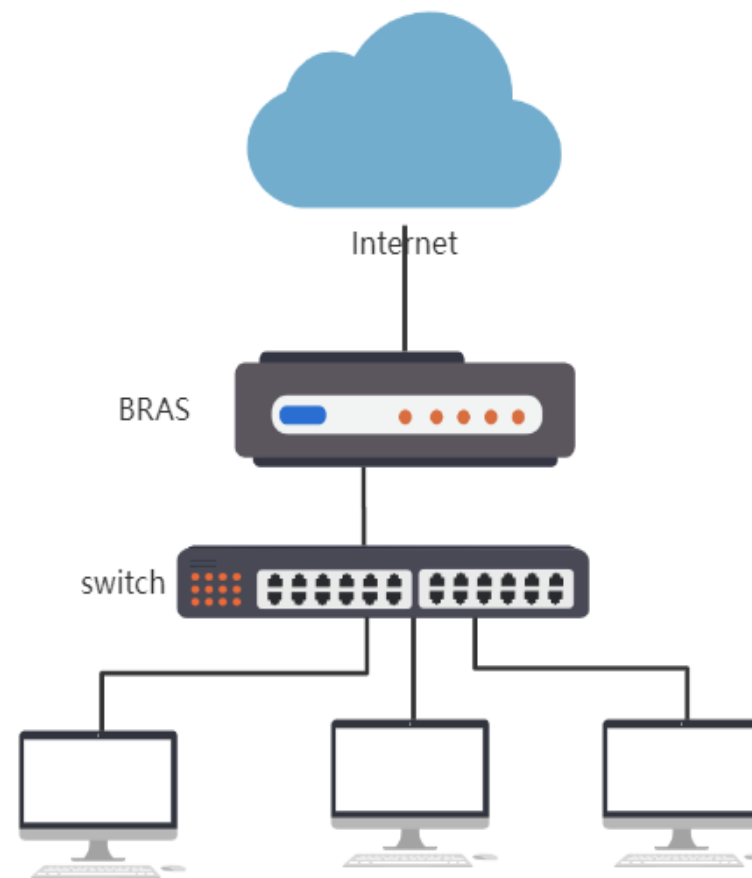
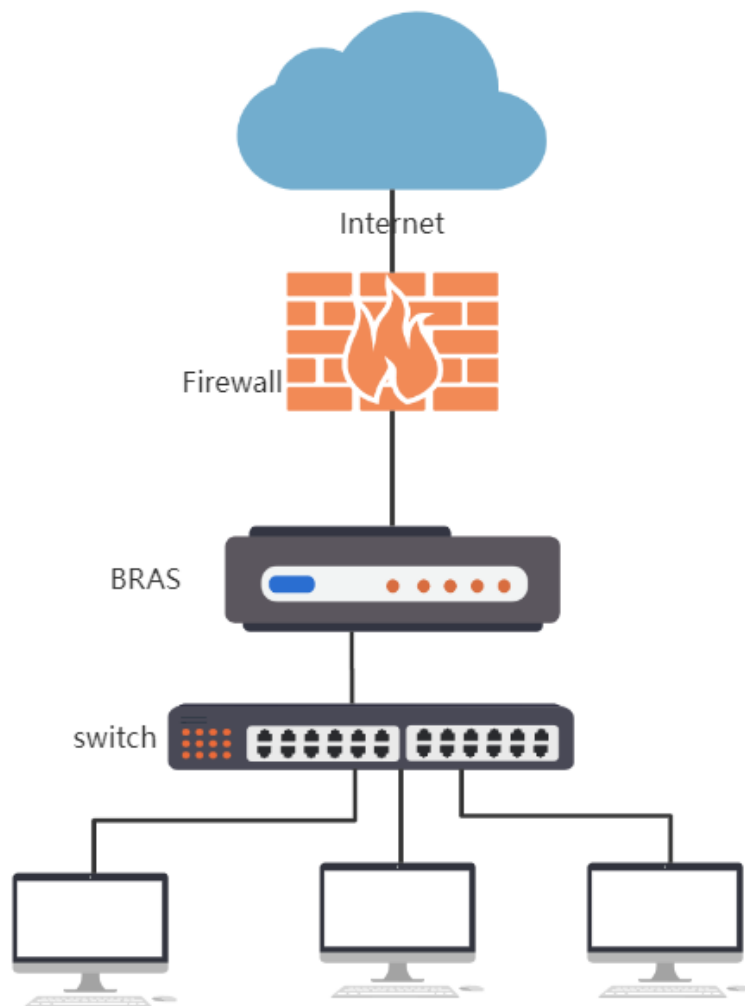
■RADIUS

RADIUS是一种C/S架构的协议，应用范围广，可扩展性高。

■cmccportal

- PPPOE认证
 - 本地认证
 - radius认证

- Portal认证
 - 本地认证
 - radius认证
 - AD域认证
 - 短信认证
 - 微信认证



■优点

- 不需要特殊客户端支持
- portal页面与用户的交互比较好

■缺点

- 必须有互联网
- 需要额外的开销
- 认证流程相对复杂

■ HTTP 302

302 Found，原始描述短语为 **Moved Temporarily**，是 HTTP 协议中的一个状态码(Status Code)。可以简单的理解为该资源原本确实存在，但已经被**临时**改变了位置；换言之，就是请求的资源暂时驻留在不同的URI下，故而除非特别指定了缓存头部指示，该状态码不可缓存。

HTTP 302

No.	Time	Source	Protocol	Destination	Length	Info
107	15.017315	172.16.16.100	TCP	17.253.39.205	78	56812→80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=904520870 TSecr=...
110	15.347909	17.253.39.205	TCP	172.16.16.100	74	80→56812 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1456 SACK_PERM=1 TSval=4...
111	15.350601	172.16.16.100	TCP	17.253.39.205	66	56812→80 [ACK] Seq=1 Ack=1 Win=131392 Len=0 TSval=904521203 TSecr=4047876966
113	15.370818	172.16.16.100	HTTP	17.253.39.205	197	GET /hotspot-detect.html HTTP/1.0
114	15.370864	17.253.39.205	HTTP	172.16.16.100	303	HTTP/1.1 302 Found
115	15.372578	172.16.16.100	TCP	17.253.39.205	66	56812→80 [ACK] Seq=132 Ack=250 Win=131136 Len=0 TSval=904521225 TSecr=4047876966
124	15.381678	172.16.16.100	TCP	17.253.39.205	66	56812→80 [FIN, ACK] Seq=132 Ack=250 Win=131136 Len=0 TSval=904521232 TSecr=404787...
256	15.702592	17.253.39.205	TCP	172.16.16.100	60	80→56812 [RST] Seq=250 Win=0 Len=0
257	15.712258	17.253.39.205	TCP	172.16.16.100	60	80→56812 [RST] Seq=250 Win=0 Len=0

```
> Frame 114: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface 0
> Ethernet II, Src: b0:f3:3d:9e:00:a0 (b0:f3:3d:9e:00:a0), Dst: Apple_30:9f:4d (20:a2:e4:30:9f:4d)
> Internet Protocol Version 4, Src: 17.253.39.205, Dst: 172.16.16.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 56812, Seq: 1, Ack: 132, Len: 249
v Hypertext Transfer Protocol
  v HTTP/1.1 302 Found\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
      Request Version: HTTP/1.1
      Status Code: 302
      Response Phrase: Found
      Location: http://192.168.0.199:8080/webauth/portal.html?ver=1.0&type=17&clientip=172.16.16.100&clientmac=20:a2:e4:30:9f:4d&paip=192.168.0.199&iarmdst=captive.apple.com/hotspot-detect.h
      Connection: close\r\n
    > Content-Length: 0\r\n
      \r\n
    [HTTP response 1/1]
    [Time since request: 0.000046000 seconds]
    [Request in frame: 113]
```

```
0040 30 32 20 46 6f 75 6e 64 0d 0a 4c 6f 63 61 74 69 02 Found ..Locati
0050 6f 6e 3a 20 68 74 74 70 3a 2f 2f 31 39 32 2e 31 on: http ://192.1
0060 36 38 2e 30 2e 31 39 39 3a 38 30 38 30 2f 77 65 68.0.199 :8080/we
0070 62 61 75 74 68 2f 70 6f 72 74 61 6c 2e 68 74 6d bauth/po rtal.htm
0080 6c 3f 76 65 72 3d 31 2e 30 26 74 79 70 65 3d 31 l?ver=1. 0&type=1
0090 37 26 63 6c 69 65 6e 74 69 70 3d 31 37 32 2e 31 7&client ip=172.1
00a0 36 2e 31 36 2e 31 30 30 26 63 6c 69 65 6e 74 6d 6.16.100 &clientm
00b0 61 63 3d 32 30 3a 61 32 3a 65 34 3a 33 30 3a 39 ac=20:a2 :e4:30:9
```

激活 Windows
转到“设置”以激活 Windows。

应用显示过滤器 ... <Ctrl-/> 表达式...

No.	Time	Source	Protocol	Destination	Length	Info
37	13.316330	10.0.0.1	portal	10.0.0.254	92	PORTAL REQ_INFO (SerNo=46568)
38	13.316434	10.0.0.254	portal	10.0.0.1	60	PORTAL ACK_INFO (SerNo=46568)
39	13.464347	10.0.0.1	portal	10.0.0.254	92	PORTAL REQ_AUTH (SerNo=46568)
40	13.464468	10.0.0.254	portal	10.0.0.1	60	PORTAL ACK_AUTH (SerNo=46568)
41	13.464470	10.0.0.1	ICMP	10.0.0.254	70	Destination unreachable (Port unreachable)
42	13.464618	b0:78:4d:0b:00:40	ARP	Broadcast	60	Gratuitous ARP for 10.0.0.254 (Request)
43	13.476362	10.0.0.1	portal	10.0.0.254	92	PORTAL REQ_INFO (SerNo=46568)
44	13.476471	10.0.0.254	portal	10.0.0.1	60	PORTAL ACK_INFO (SerNo=46568)
45	13.635675	10.0.0.1	portal	10.0.0.254	92	PORTAL REQ_AUTH (SerNo=46568)
46	13.635808	10.0.0.254	portal	10.0.0.1	60	PORTAL ACK_AUTH (SerNo=46568)

> Frame 39: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)

> Ethernet II, Src: 50:9a:4c:91:57:a6 (50:9a:4c:91:57:a6), Dst: b0:78:4d:0b:00:40 (b0:78:4d:0b:00:40)

> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.254

> User Datagram Protocol, Src Port: 41758, Dst Port: 2000

▼ Portal Protocol

Version: 1

Type: REQ_AUTH

Pap/Chap: PAP

Rsv: 0

SerialNo: 46568

ReqId: 0

UserIP: 172.16.1.180

UserPort: 0

ErrCode: 0

AttrNum: 3

Attribute Value 参数如下:

User-Name: 17866550669@net

Pap-Password: 88888888

```

0000  b0 78 4d 0b 00 40 50 9a 4c 91 57 a6 08 00 45 00  .XM..@P. L.W...E.
0010  00 4e 5c 87 00 00 40 11 00 00 0a 00 00 01 0a 00  .N\...@. ....
0020  00 fe a3 1e 07 d0 00 3a 60 a3 01 03 01 00 b5 e8  .....:  .
0030  00 00 ac 10 01 b4 00 00 00 03 01 11 31 37 38 36  ..... 1786
0040  36 35 35 30 36 36 39 40 6e 65 74 02 0a 38 38 38  6550669@ net..888
0050  38 38 38 38 38 fe 07 35 30 30 2e 30              88888..5 00.0

```

Wireshark Lua text (_ws.lua.text), 1 字节

分组: 1758 · 已显示: 1758 (100.0%) · 加载时间: 0:0.93 配置文件: Default

激活 Windows
转到“设置”以激活 Windows。

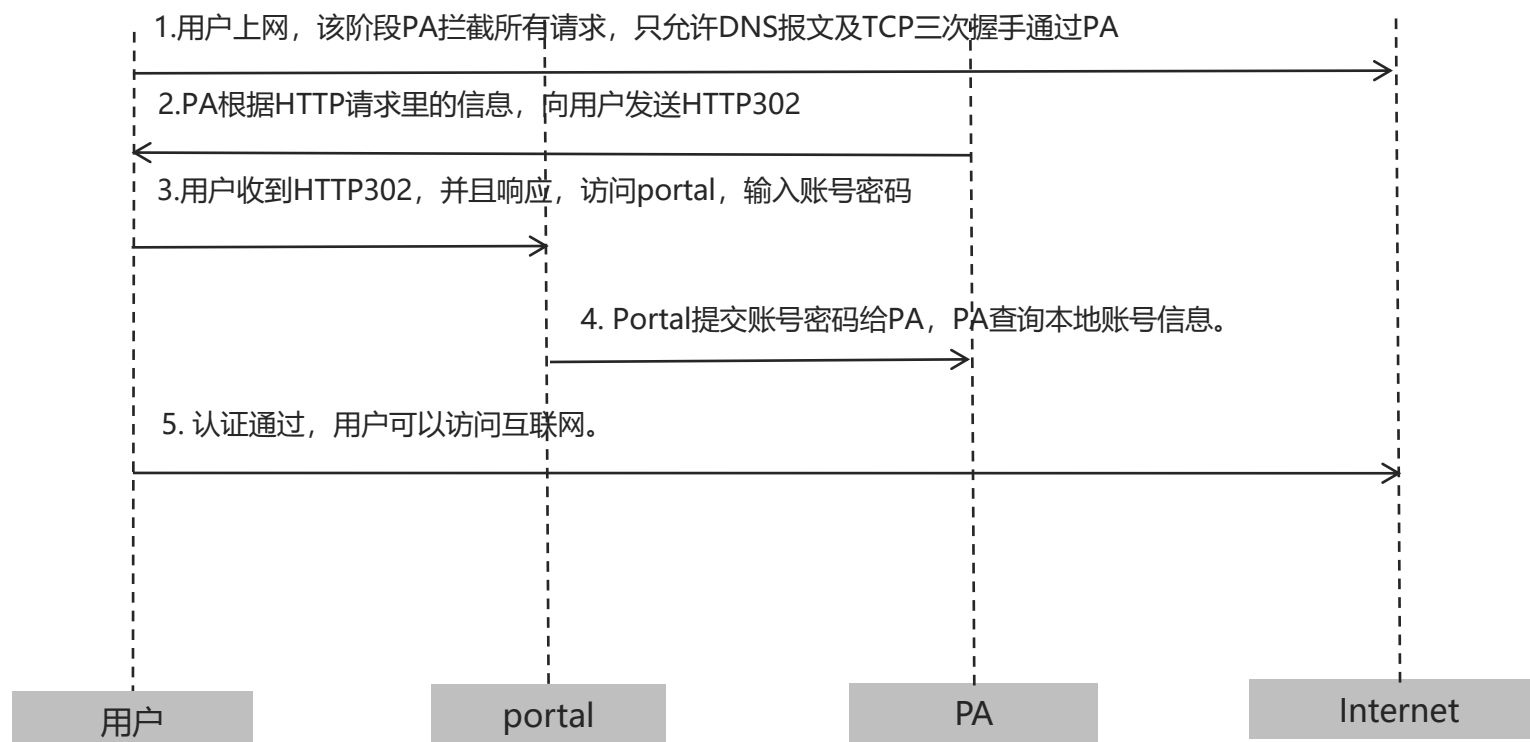


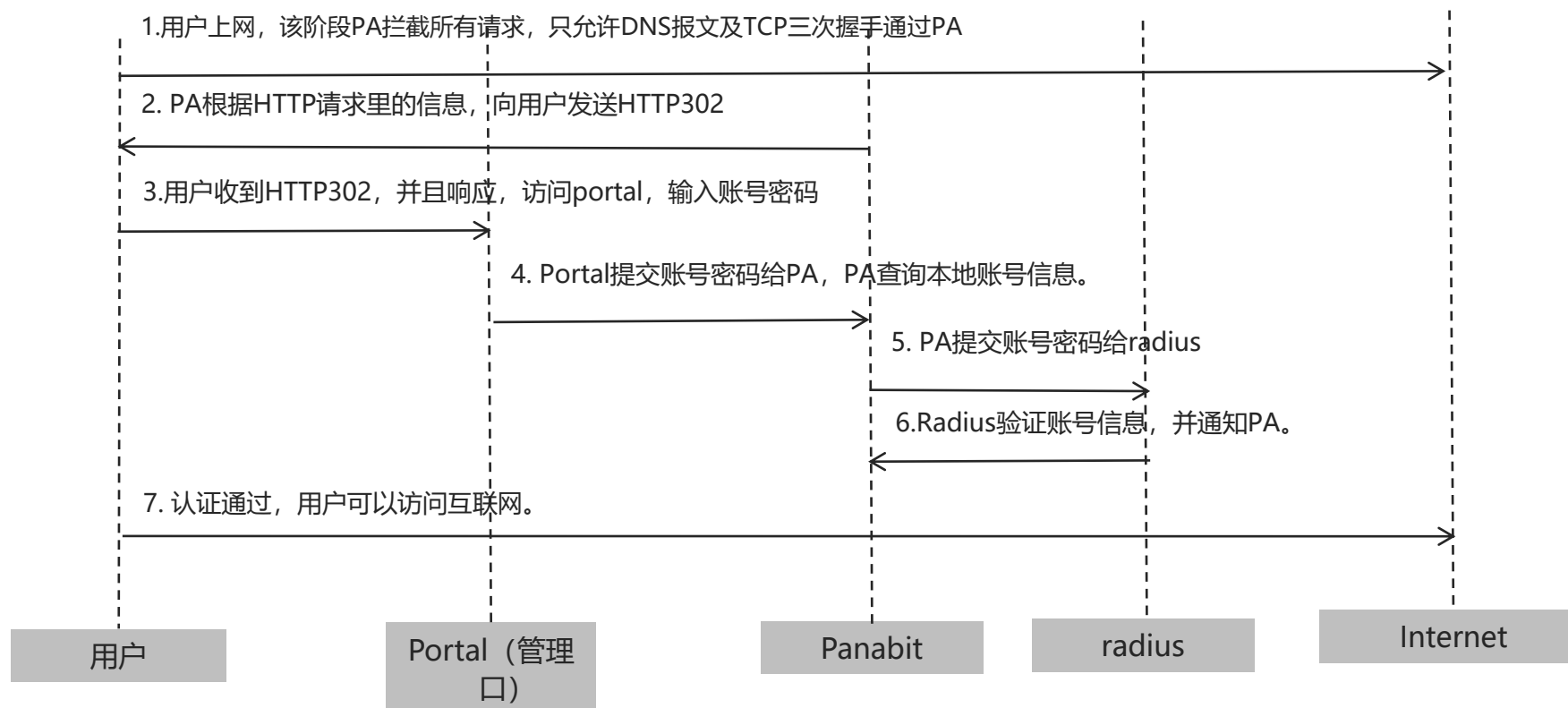
基本参数

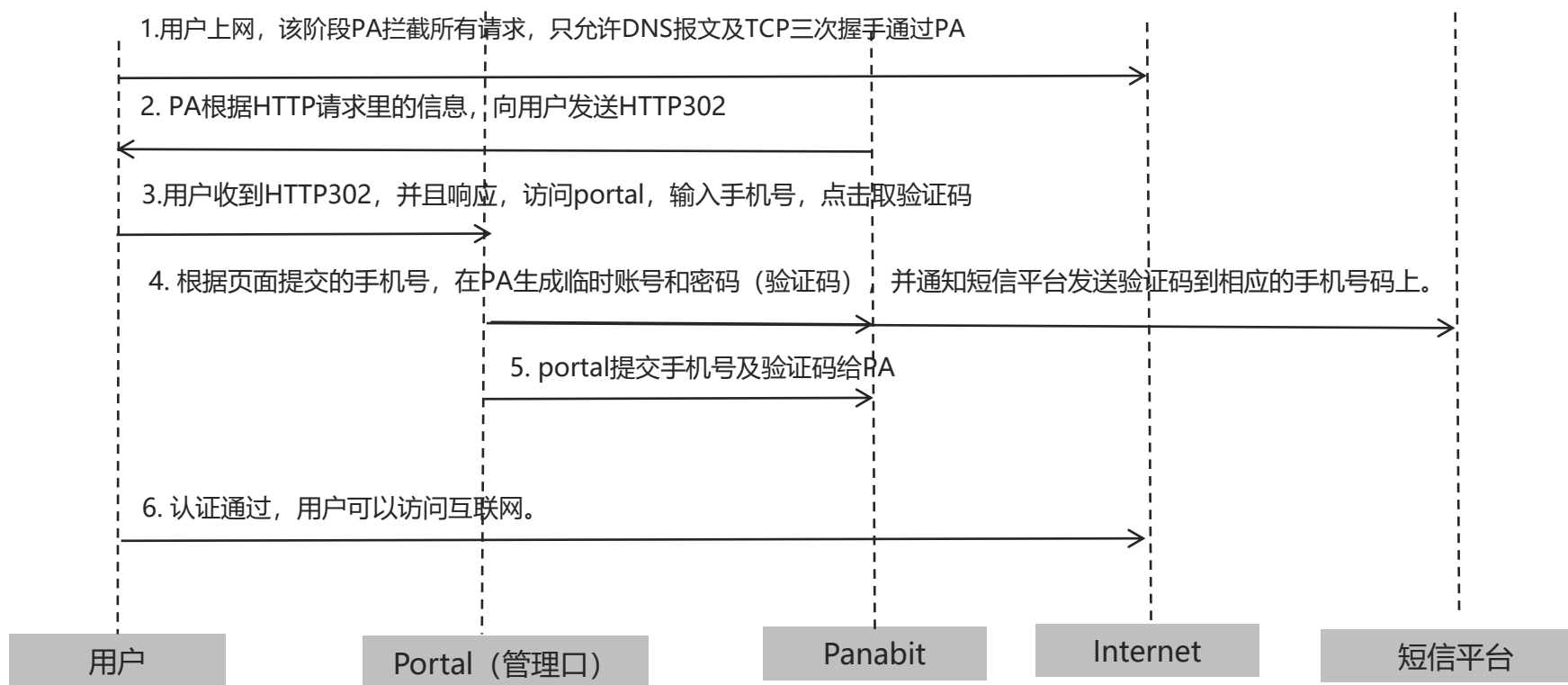
Web认证	<div>打开</div>
去掉URL中的客户端IP	<div>关闭</div>
HTTPS跳转	<div>关闭</div>
免认证IP	<div>放通</div> <div>[编辑IP]</div>
免认证MAC地址	<div>0</div> <div>[编辑MAC]</div>
免认证协议	<div></div> <div>[选择应用 清除]</div>
成功后显示页面	<div></div>
登陆后弹出注销页	<div>否</div> <div>注销时检查MAC地址是否与IP匹配:</div> <div>否</div>
允许自动登陆选项	<div>否</div> <div>记住密码超时时间:</div> <div>7</div> <div>天内不登陆, 需重新输入帐号密码。(0表示无记住密码选项)</div>
帐号登陆错误限制	<div></div> <div>秒内错误3次, 拒绝登陆。(0: 表示不限制。)</div>
多帐号登陆限制	<div>否</div> <div>本地、RADIUS或AD/LDAP帐号登陆时是否先将已在线的帐号踢下线。是: 表示踢; 默认: 为否。</div>
关闭修改密码功能	<div>否</div> <div>关闭后, 用户将不能在WEB认证页面中修改帐号的密码。若当密码为“123456”时强制修改</div> <div>否</div>
修改密码后重新登陆帐号	<div>否</div>
不允许找回密码	<div>否</div> <div>目前只支持对接RAAS时有效, 需要在radius.conf配置中增加“api_forgot” API接口后支持。</div>
PortalURL	<div>http://192.168.8.58:8080/webauth/portal.html?ver=1.0</div> <div>认证入口URL, 默认为本地界面。</div>
PortalIP	<div></div> <div>授权安全管理的IP, 若无特殊需要, 请填写上面URL的IP地址。</div>

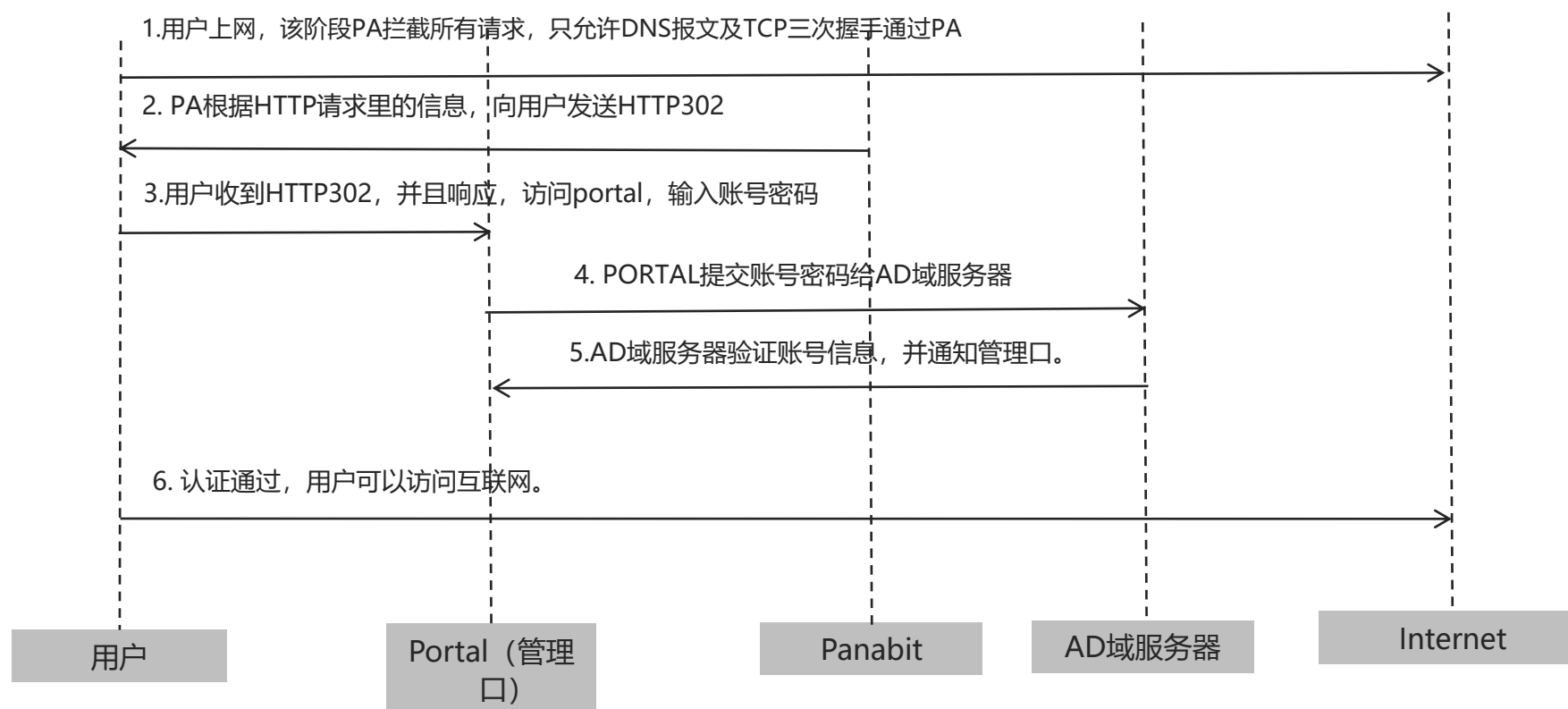
帐号密码认证

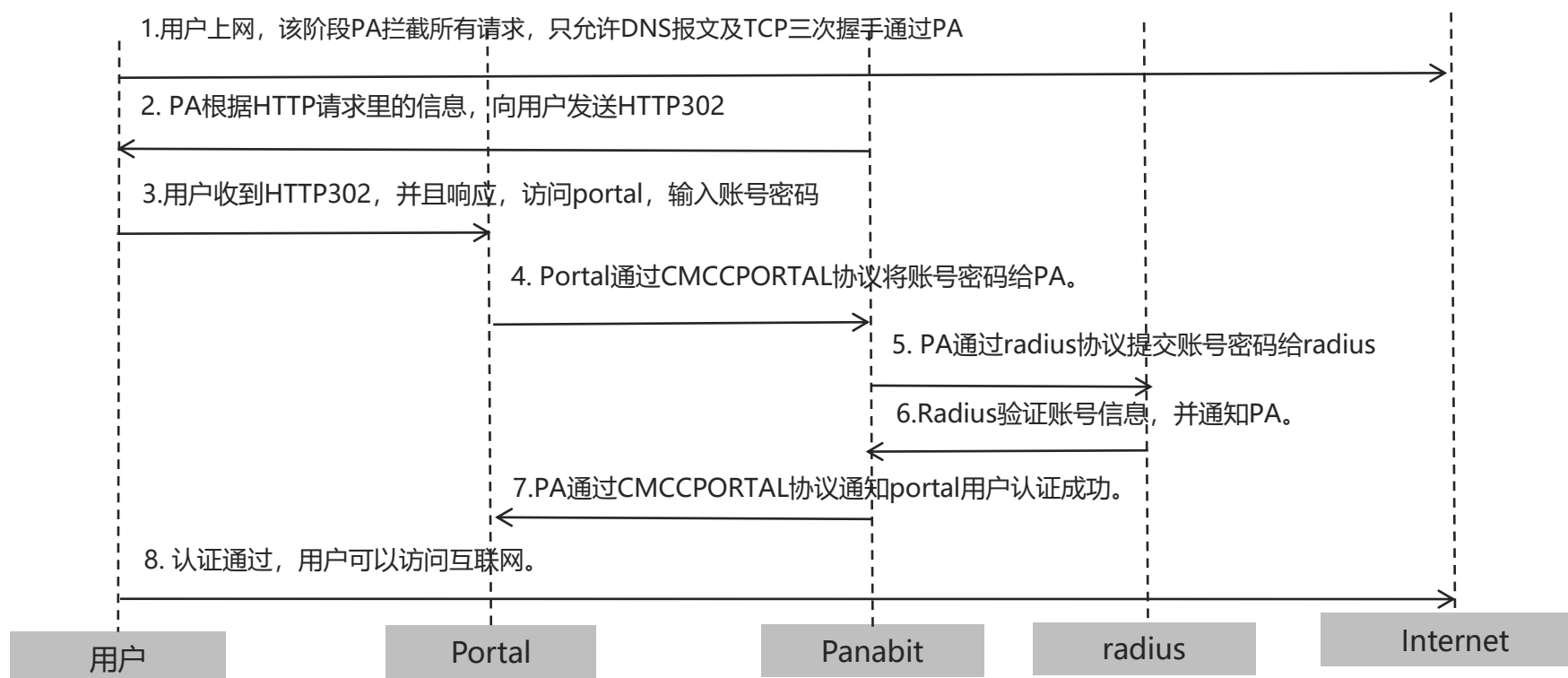
<div><div>本地帐号</div><div><div>RADIUS</div></div><div>AD/LDAP</div><div>手机短信认证</div></div>	<div>基于本地帐号的WEB认证。<div>附加手机短信认证</div></div> <div><div>请选择认证服务:</div><div>raas</div><div>查看服务明细</div><div>附加手机短信认证</div></div> <div><div>服务器地址:</div><div>ldap:/</div><div>0.0.0.0</div><div>端口:</div><div>389</div><div>(编辑配置)</div><div>(1~65535, LDAP默认端口为: 389)</div></div> <div><div>短信平台:</div><div>阿里云</div><div>编辑配置</div><div>白名单登陆</div><div>编辑白名单</div><div>最大在线数:</div><div>1</div></div>
---	--

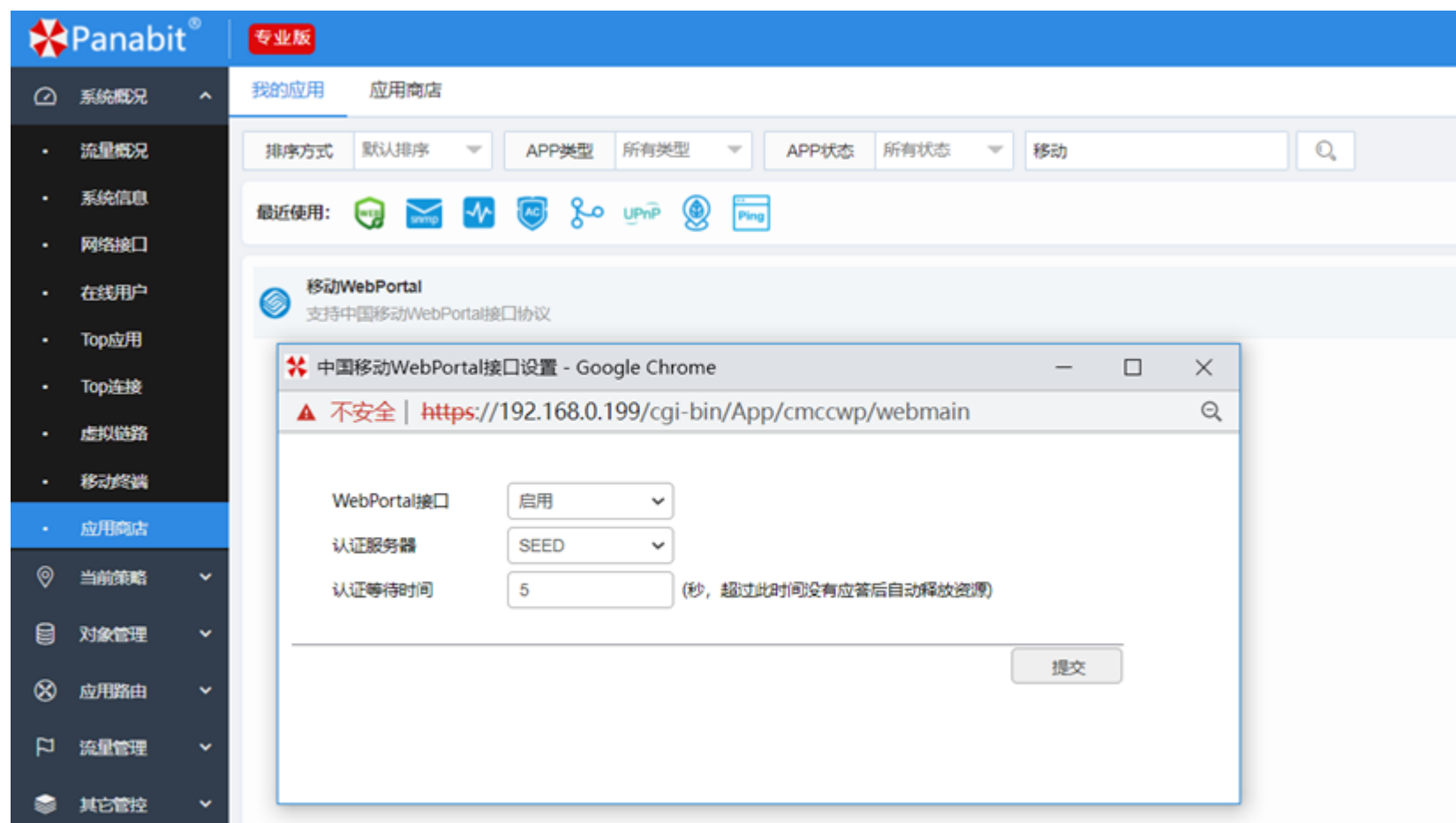










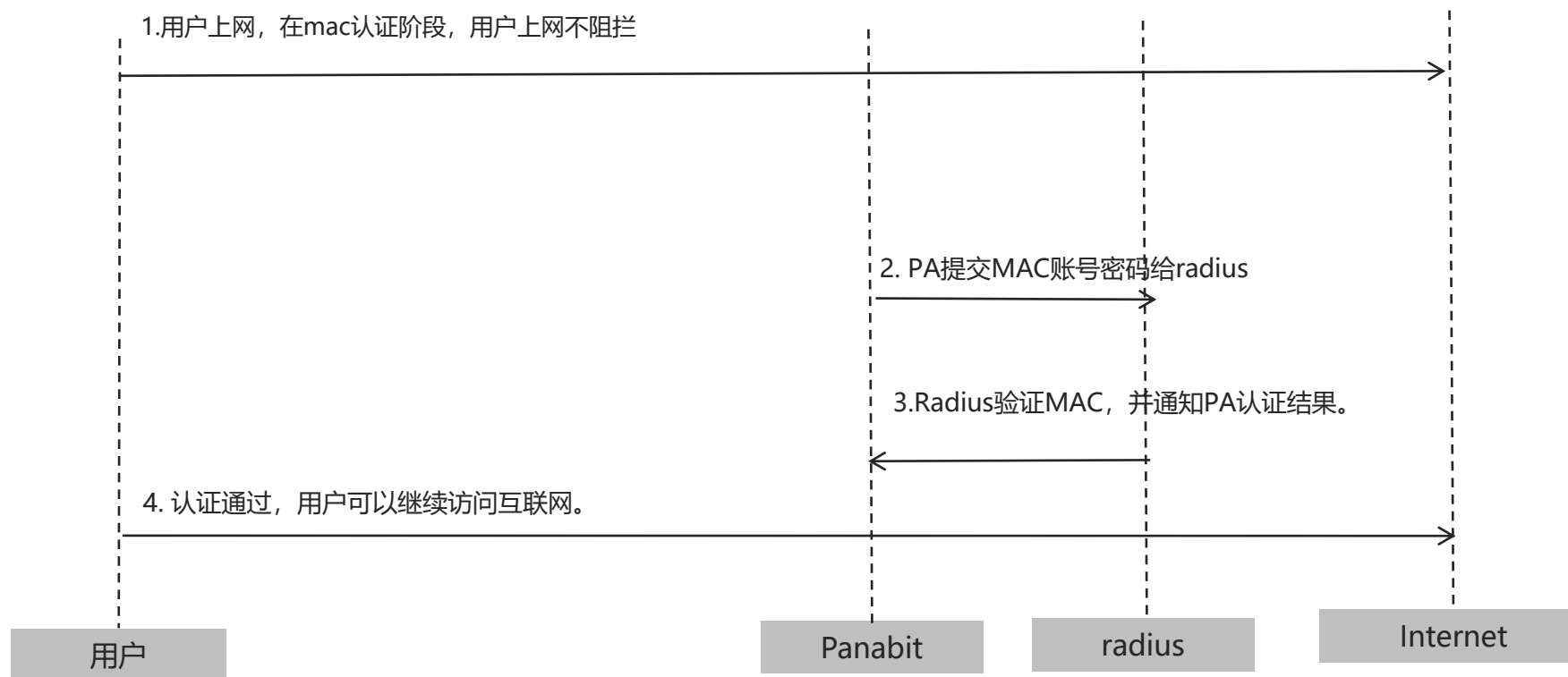


在很多认证场景中，用户希望实现无感知认证。即只有首次登录需要进行web 认证，再次使用时就不需要再输入用户名和密码认证了，即使用户异常掉线，如：关机重启、意外断网或离开校园无线网区域，当无线终端再次进入无线网覆盖区域时均可自动认证，实现用户永远在线。这一过程由系统自动完成，对用户“无感知”

开个命令 `floweye macauth config enable=1`

状态查看 `floweye macauth stat`

参数调整 `floweye macauth config retry=3 interval=5`



■ 跨三层取MAC



■ DHCP SNIF

命令行输入

```
floweye dhcpsnif4 config enable=1
```

■优点

- 用户状态明确，计费灵活
- 可以避免内网地址冲突，ARP欺骗
- 认证流程标准且简单

■缺点

- 需要客户端支持
- 必须是二层网络架构

■优点

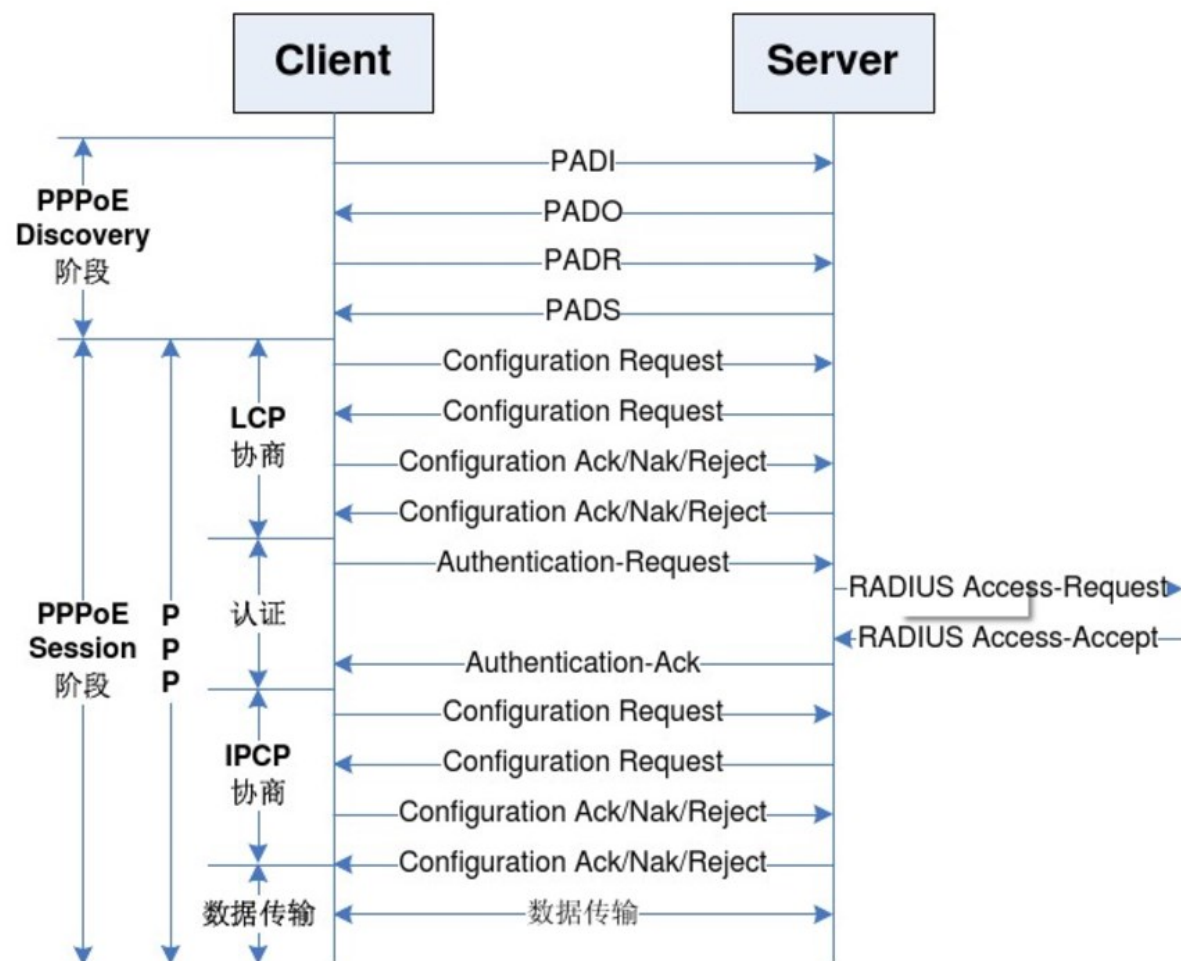
- 用户状态明确，计费灵活
- 可以避免内网地址冲突，ARP欺骗
- 认证流程标准且简单

■缺点

- 需要客户端支持
- 必须是二层网络架构

- PPPoE分成两个阶段：

1. PPPoE发现阶段；
2. PPPoE会话阶段。



Discovery阶段由4个步骤组成。完成之后通信双方都知道了PPPoE SESSION_ID以及对方以太网地址，它们共同定义了唯一的PPPoE会话。这些步骤包括：

- ◆ client广播一个**Initiation** (PADI) 数据包 (以请求建立链路)
- ◆ 一个或多个server发送**Offer** (PADO) 数据包
- ◆ client发送单播**SessionRequest**(PADR)数据包
- ◆ server发送Session-Confirmation (PADS) 数据包

至此，PPPoE会话建立，后续进入PPP会话阶段。

思考：PPPoE Discovery阶段的主要任务是什么？

pppoed						
No.	Time	Source	Destination	Protocol	Length	Info
497	35.018075	f8:59:71:1c:c0:28	Broadcast	PPPoED	42	Active Discovery Initiation (PADI)
498	35.020135	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPPoED	67	Active Discovery Offer (PADO) AC-Name='AAA'
499	35.020171	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPPoED	42	Active Discovery Request (PADR)
Frame 497: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
Ethernet II, Src: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
Destination: Broadcast (ff:ff:ff:ff:ff:ff)						
Source: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)						
Type: PPPoE Discovery (0x8863)						
PPP-over-Ethernet Discovery						
0001 = Version: 1						
.... 0001 = Type: 1						
Code: Active Discovery Initiation (PADI) (0x09)						
Session ID: 0x0000						
Payload Length: 22						
PPPoE Tags						
Service-Name: pa						
Host-Uniq: 040000000000000007000000						

client发送广播地址的PADI数据包

PADI数据包包含Service-Name的TAG。它表示主机请求的服务（该TAG可选，而且只能有一个

No.	Time	Source	Destination	Protocol	Length	Info
497	35.018075	f8:59:71:1c:c0:28	Broadcast	PPPoED	42	Active Discovery Initiation (PADI)
498	35.020135	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPPoED	67	Active Discovery Offer (PADO) AC-Name='AAA'
499	35.020171	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPPoED	42	Active Discovery Request (PADR)
> Frame 498: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0						
✓ Ethernet II, Src: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50), Dst: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)						
> Destination: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)						
> Source: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50)						
Type: PPPoE Discovery (0x8863)						
✓ PPP-over-Ethernet Discovery						
0001 = Version: 1						
.... 0001 = Type: 1						
Code: Active Discovery Offer (PADO) (0x07)						
Session ID: 0x0000						
Payload Length: 29						
✓ PPPoE Tags						
Service-Name: pa						
Host-Uniq: 040000000000000070000000						
AC-Name: AAA						

如果SERVER能够为收到的PADI请求提供服务，它将通过发送一个PADO数据包来做出应答。

DESTINATION_ADDR为发送PADI的主机的单播地址

含有与PADI相同的Service-Name的TAG

AC-Name的TAG（包含了SERVER的名字）

No.	Time	Source	Destination	Protocol	Length	Info
499	35.020171	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPPoED	42	Active Discovery Request (PADR)
500	35.021684	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPPoED	60	Active Discovery Session-confirmation (PADS)
513	35.087699	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPPoED	60	Active Discovery Terminate (PADT)

> Frame 499: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

✓ Ethernet II, Src: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28), Dst: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50)

- > Destination: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50)
- > Source: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)
- Type: PPPoE Discovery (0x8863)

✓ PPP-over-Ethernet Discovery

- 0001 = Version: 1
- 0001 = Type: 1
- Code: Active Discovery Request (PADR) (0x19)
- Session ID: 0x0000
- Payload Length: 22
- ✓ PPPoE Tags
 - Service-Name: pa

Host-Uniq: 040000000000000008000000

由于PADI是广播的,网络中有多个SERVER,那么client可能收到不止一个PADO,它将审查接收到的所有PADO并从中选择一个。可以根据其中的AC-Name或PADO所提供的服务来作出选择。然后client向选中的SERVER发送一个PADR数据包。其中, DESTINATION_ADDR为发送PADO的SERVER的单播地址, CODE域设置为0x19, SESSION_ID为0x0000。包含且仅包含一个为Service-Name的TAG, 表明client请求的服务

No.	Time	Source	Destination	Protocol	Length	Info
499	35.020171	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPPoED	42	Active Discovery Request (PADR)
500	35.021684	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPPoED	60	Active Discovery Session-confirmation (PADS)
513	35.087699	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPPoED	60	Active Discovery Terminate (PADT)

> Frame 500: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

✓ Ethernet II, Src: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50), Dst: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)

> Destination: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)
 > Source: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50)
 Type: PPPoE Discovery (0x8863)

✓ PPP-over-Ethernet Discovery

0001 = Version: 1
 0001 = Type: 1
 Code: Active Discovery Session-confirmation (PADS) (0x65)
 Session ID: 0x0002
 Payload Length: 22

✓ PPPoE Tags

Service-Name: pa
 Host-Uniq: 040000000000000008000000

当SERVER收到一个PADR数据包，它就准备开始一个PPP会话。它为PPPoE会话创建一个唯一的SESSION_ID并用一个PADS数据包来给主机作出响应。DESTINATION_ADDR域为发送PADR数据包的主机的单播以太网地址，CODE域设置为0x65，SESSION_ID必须设置为所创建好的PPPoE会话标识符。至此，PPPoE Discovery 阶段结束，准备进入PPP会话阶段。PPPoE Discovery 阶段的两大任务：1寻找可用的SERVER;2,得到SESSION ID，开始PPP会话；



1. LCP协商阶段:

LCP = Link Control Protocol, 链路控制协议

此阶段主要是协商链路的一些参数, 如最大接收单元MRU、Magic Number, 以及后续认证时使用的协议等;

2. 认证阶段:

此阶段服务器端将验证客户端的合法性。最常见的两种就是PAP和CHAP;

1. PAP认证: 发送的认证信息是明文, 可以通过抓包工具看到用户名、密码;

2. CHAP认证: 发送的认证信息是密文, 抓包工具无法解析出来真正的用户名、密码。

3. IPCP阶段:

此阶段进行IP、DNS、WINS等的协商;

4. 数据传输

上述任一阶段失败都会导致协议终止。

如果都成功, 则可以开始进行IP层的通信了;

- 1, PPP的过程中client与SERVER任何一方都可以主动发起request来协商参数
- 2, 协商过程中主要有三个动作:
 - A) 应答ACK, 表示同意
 - B) 应答NAK, 表示不同意, 但是有商量的余地, 并且告诉对方自己能接受的值
 - C) 应答reject, 表示完全拒绝, 不认识的属性, 没有商量的余地。

» IPCP Request数据包截图

1619	32.912908	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	56 Configuration Request
1621	33.116264	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPP LCP	60 Protocol Reject
1622	33.116264	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPP IPCP	60 Configuration Request
1623	33.116264	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPP IPCP	60 Configuration Reject
1624	33.116403	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	32 Configuration Ack
1625	33.116489	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	44 Configuration Request

- > Frame 1619: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
- > Ethernet II, Src: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28), Dst: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50)
- > PPP-over-Ethernet Session
- ✓ Point-to-Point Protocol
 - Protocol: Internet Protocol Control Protocol (0x8021)
- ✓ PPP IP Control Protocol
 - Code: Configuration Request (1)
 - Identifier: 6 (0x06)
 - Length: 34
 - ✓ Options: (30 bytes), IP address, Primary DNS Server IP Address, Primary NBNS Server IP Address, Secondary DNS Server IP Address, Se
 - IP address: 0.0.0.0
 - Primary DNS Server IP Address: 0.0.0.0
 - Primary NBNS Server IP Address: 0.0.0.0
 - Secondary DNS Server IP Address: 0.0.0.0
 - Secondary NBNS Server IP Address: 0.0.0.0

Client请求若干参数



IPCP Reject数据包截图



1623	33.116264	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPP IPCP	60 Configuration Reject
1624	33.116403	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	32 Configuration Ack
1625	33.116489	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	44 Configuration Request

>

Frame 1623: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

>

Ethernet II, Src: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50), Dst: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)

>

PPP-over-Ethernet Session

▼

Point-to-Point Protocol

Protocol: Internet Protocol Control Protocol (0x8021)

▼

PPP IP Control Protocol

Code: Configuration Reject (4)

Identifier: 6 (0x06)

Length: 16

▼

Options: (12 bytes), Primary NBNS Server IP Address, Secondary NBNS Server IP Address

>

Primary NBNS Server IP Address: 0.0.0.0

>

Secondary NBNS Server IP Address: 0.0.0.0

SERVER不认识NBNS，应答reject，完全拒绝这两个参数

- [-] PPP-over-Ethernet Session
 - 0001 = Version: 1
 - 0001 = Type: 1
 - Code: Session Data (0x00)
 - Session ID: 0x0031
 - Payload Length: 24
- [-] Point-to-Point Protocol
 - Protocol: Internet Protocol Control Protocol (0x8021)
- [-] PPP IP Control Protocol
 - Code: Configuration Request (1)
 - Identifier: 8 (0x08)
 - Length: 22
 - [-] Options: (18 bytes), IP address, Primary DNS Server IP Address, Secondary DNS Server IP Address
 - + IP address: 0.0.0.0
 - + Primary DNS Server IP Address: 0.0.0.0
 - + Secondary DNS Server IP Address: 0.0.0.0

Client收到reject后，知道SERVER不支持NBNS，再次协商请求分配IP与DNS。

1625	33.116489	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	44 Configuration Request
1631	33.330359	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPP IPCP	60 Configuration Nak
1632	33.330460	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	44 Configuration Request

- > Frame 1631: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- > Ethernet II, Src: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50), Dst: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)
- > PPP-over-Ethernet Session
- ✓ Point-to-Point Protocol
 - Protocol: Internet Protocol Control Protocol (0x8021)
- ✓ PPP IP Control Protocol
 - Code: Configuration Nak (3)
 - Identifier: / (0x0/)
 - Length: 22
 - ✓ Options: (18 bytes), IP address, Primary DNS Server IP Address, Secondary DNS Server IP Address
 - > IP address: 12.12.12.2
 - > Primary DNS Server IP Address: 114.114.114.114
 - > Secondary DNS Server IP Address: 8.8.8.8

SERVER收到request, 但不同意0.0.0.0这个值, 发送NAK, 然后告诉client可以有这些值。

1632	33.330460	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPP IPCP	44 Configuration Request
1637	33.552072	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPP IPCP	60 Configuration Ack

- > Frame 1632: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface 0
- > Ethernet II, Src: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28), Dst: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50)
- > PPP-over-Ethernet Session
- ▼ Point-to-Point Protocol
 - Protocol: Internet Protocol Control Protocol (0x8021)
- ▼ PPP IP Control Protocol
 - Code: Configuration Request (1)
 - Identifier: 8 (0x08)
 - Length: 22
 - ▼ Options: (18 bytes), IP address, Primary DNS Server IP Address, Secondary DNS Server IP Address
 - > IP address: 12.12.12.2
 - > Primary DNS Server IP Address: 114.114.114.114
 - > Secondary DNS Server IP Address: 8.8.8.8

Client收到SEVER的NAK，按照SERVER的指示，请求这些IP和DNS值

1637	33.552072	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPP IPCP	60 Configuration Ack
> Frame 1637: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0					
> Ethernet II, Src: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50), Dst: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28)					
> PPP-over-Ethernet Session					
v Point-to-Point Protocol					
Protocol: Internet Protocol Control Protocol (0x8021)					
v PPP IP Control Protocol					
Code: Configuration Ack (2)					
Identifier: 8 (0x08)					
Length: 22					
v Options: (18 bytes), IP address, Primary DNS Server IP Address, Secondary DNS Server IP Address					
> IP address: 12.12.12.2					
> Primary DNS Server IP Address: 114.114.114.114					
> Secondary DNS Server IP Address: 8.8.8.8					

SERVER同意所有参数，IPCP阶段结束，开始IP层会话。



165	7.897918	f8:59:71:1c:c0:28	b0:dc:b2:cb:00:50	PPPoED	20 Active Discovery Terminate (PADT)
166	7.899100	b0:dc:b2:cb:00:50	f8:59:71:1c:c0:28	PPPoED	60 Active Discovery Terminate (PADT)

> Frame 165: 20 bytes on wire (160 bits), 20 bytes captured (160 bits) on interface 0

> Ethernet II, Src: f8:59:71:1c:c0:28 (f8:59:71:1c:c0:28), Dst: b0:dc:b2:cb:00:50 (b0:dc:b2:cb:00:50)

> PPP-over-Ethernet Discovery

0001 = Version: 1

.... 0001 = Type: 1

Code: Active Discovery Terminate (PADT) (0xa7)

Session ID: 0x0002

Payload Length: 0

这种数据包可以在会话建立以后的任意时刻发送，表明PPPoE会话已经终止。它可以由client或SERVER发送，DESTINATION_ADDR域为单播以太网地址，CODE域设置为0xa7，SESSION_ID设置为将要终止的会话的SESSION_ID，这种数据包不需要任何TAG。

- 1) SERVER应该不时地向client发送回声请求 (Echo-Request) 数据包, 以确定会话的状态。否则如果client在 (比如停电, 死机) 没有发送结束请求 (Terminate-Request) 数据包的情况下终止会话, 则SERVER将无法得知该会话已经 “死去”
- 2) PPPoE的最大接收单元(MRU)不允许超过1492。因为以太网的最大净载为1500字节, 而PPPoE头部为6个字节, PPP Protocol-ID为2个字节, 所以PPP的MTU不允许超过1492



PPPOE SERVER配置



专业版

系统概况

当前策略

对象管理

应用路由

流量管理

其它管控

用户认证

• 账号管理

• 在线用户

• PPPOE

• 拨号退出

• 下线日志

参数设置

服务列表

PPPOE接入服务

启用

缓存流量限速

限速

仅当使用缓存牵引的时候才有效

MAC自动绑定

不启用

此选项仅对本地账号有用,如果启用,在第一次登陆时自动绑定MAC和账号

PPPOE代理限速

不限速

当启用时,可以根据RADIUS下发参数或地址池配置对代理用户限速

客户端心跳保持

10

秒,0表示不保持心跳

过期用户在线时间

600

秒,用户过期后允许在线的时间

确定

系统概况

当前策略

对象管理

应用路由

流量管理

其它管控

用户认证

账号管理

在线用户

PPPOE

拨号退出

下线日志

页面通知

PPPOE代拨

PPPOE旁路

应用识别

系统维护

系统概况

当前策略

对象管理

应用路由

流量管理

其它管控

用户认证

账号管理

在线用户

PPPOE

拨号退出

下线日志

页面通知

PPPOE代拨

PPPOE旁路

应用识别

系统维护

专业版

参数设置

服务列表

自动刷新

10秒

关键字搜索

删除

添加

ID	名称	网络接口	服务	网关地址	DNS	VLAN	MTU	认证方式	用户组	RADIUS	在线用户	流入速率	流出速率	备注	操作
1	添加PPPOE服务器										0/0	0	0		<div>Create</div>

服务器名

PPP-SERVER

物理网卡

em1

PPPOE网关

192.168.1.1

服务

如果不为空, 则只接受同名服务的客户端请求

VLAN

0

格式100,或100-200,不填或填0表示接受任意VLAN客户端请求

MTU

1480

DNS1

114.114.114.114

DNS2

8.8.8.8

认证方式

本地认证

最大接入用户

最大允许接入的用户数,0表示不限制

可服务用户

所有用户

MAC地址的最后两个字节判断奇偶

备注

确定

取消

激活 Windows

转到“设置”以激活 Windows。



■本地认证

■radius认证

■先本地后radius认证

■免认证



■PPPOE代理

■PPPOE旁路

两者都是跨bras的认证需求，利用PPPOE认证流程不同阶段的特性实现



RADIUS认证报文(access)

- 1) user-name, 用户名;
- 2) user-password, 密码;
- 3) acc-session-id, 会话ID ;
- 4) NAS-Identifer, NAS标识;
- 5) NAS-ip-address, NAS ip;



Access-Request

radius						
No.	Time	Source	Protocol	Destination	Length	Info
78	14.806665	192.168.8.1	RADIUS	192.168.8.220	151	Access-Request(1) (id=32, l=109)
79	14.807361	192.168.8.220	RADIUS	192.168.8.1	77	Access-Accept(2) (id=32, l=35)
92	14.809827	192.168.8.1	RADIUS	192.168.8.220	199	Accounting-Request(4) (id=1, l=157)
93	14.810469	192.168.8.220	RADIUS	192.168.8.1	62	Accounting-Response(5) (id=1, l=20)

> Frame 78: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
> Ethernet II, Src: b0:f3:3d:9e:00:50 (b0:f3:3d:9e:00:50), Dst: Vmware_71:a1:b2 (00:0c:29:71:a1:b2)
> Internet Protocol Version 4, Src: 192.168.8.1, Dst: 192.168.8.220
> User Datagram Protocol, Src Port: 50000, Dst Port: 1812

▼ RADIUS Protocol

Code: Access-Request (1)
Packet identifier: 0x20 (32)
Length: 109
Authenticator: 4d830000e175ac21b2596f410aa81f97
[\[The response to this request is in frame 79\]](#)

▼ Attribute Value Pairs

> AVP: l=5 t=User-Name(1): lu0
> AVP: l=18 t=User-Password(2): Encrypted
> AVP: l=19 t=Calling-Station-Id(31): 54:e1:ad:20:7f:b8
> AVP: l=7 t=Called-Station-Id(30): PPP0E
> AVP: l=6 t=NAS-IP-Address(4): 192.168.8.1
> AVP: l=19 t=Acct-Session-Id(44): PA_00031_e42ce0a7
> AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
> AVP: l=9 t=NAS-Identifier(32): Panabit

下面几个RADIUS属性影响Panabit分配IP地址行为：

- 1) Framed-IP-Address: Panabit使用这个属性来作为客户的IP地址，如果没有这个属性，就看下面这个属性；
- 2) Framed-Pool: 这个属性是Panabit的64个地址池中的某一个（名称或编号均可）；如果没有Framed-IP-Address属性，Panabit就从这个属性指定的地址池中分配IP给客户；
- 3) 如果上面两个属性都没有，Panabit就从PPPOE SERVER中的默认地址池分配一个IP给客户；

总而言之：先根据RADIUS指示进行分配，RADIUS没指示的话，就根据Panabit自己的设置分配



radius						
No.	Time	Source	Protocol	Destination	Length	Info
78	14.806665	192.168.8.1	RADIUS	192.168.8.220	151	Access-Request(1) (id=32, l=109)
79	14.807361	192.168.8.220	RADIUS	192.168.8.1	77	Access-Accept(2) (id=32, l=35)
92	14.809827	192.168.8.1	RADIUS	192.168.8.220	199	Accounting-Request(4) (id=1, l=157)
93	14.810469	192.168.8.220	RADIUS	192.168.8.1	62	Accounting-Response(5) (id=1, l=20)

> Frame 79: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

> Ethernet II, Src: Vmware_71:a1:b2 (00:0c:29:71:a1:b2), Dst: b0:f3:3d:9e:00:50 (b0:f3:3d:9e:00:50)

> Internet Protocol Version 4, Src: 192.168.8.220, Dst: 192.168.8.1

> User Datagram Protocol, Src Port: 1812, Dst Port: 50000

▼ RADIUS Protocol

Code: Access-Accept (2)

Packet identifier: 0x20 (32)

Length: 35

Authenticator: ee5315a3d120f011b08b97cc8fbd003f

[\[This is a response to a request in frame 78\]](#)

[Time from request: 0.000696000 seconds]

▼ Attribute Value Pairs

> AVP: l=6 t=Session-Timeout(27): 305686319

> AVP: l=6 t=Acct-Interim-Interval(85): 60

> AVP: l=3 t=Framed-Pool(88): 2



radius						
No.	Time	Source	Protocol	Destination	Length	Info
109	23.365779	192.168.8.1	RADIUS	192.168.8.220	151	Access-Request(1) (id=20, l=109)
110	23.367456	192.168.8.220	RADIUS	192.168.8.1	122	Access-Accept(2) (id=20, l=80)
123	23.369339	192.168.8.1	RADIUS	192.168.8.220	199	Accounting-Request(4) (id=1, l=157)
124	23.369880	192.168.8.220	RADIUS	192.168.8.1	62	Accounting-Response(5) (id=1, l=20)

> Frame 110: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0

> Ethernet II, Src: Vmware_71:a1:b2 (00:0c:29:71:a1:b2), Dst: b0:f3:3d:9e:00:50 (b0:f3:3d:9e:00:50)

> Internet Protocol Version 4, Src: 192.168.8.220, Dst: 192.168.8.1

> User Datagram Protocol, Src Port: 1812, Dst Port: 50000

▼ RADIUS Protocol

Code: Access-Accept (2)

Packet identifier: 0x14 (20)

Length: 80

Authenticator: 36d4765cb3392f826bb5e414f247c85e

[\[This is a response to a request in frame 109\]](#)

[Time from request: 0.001677000 seconds]

▼ Attribute Value Pairs

> AVP: l=6 t=Session-Timeout(27): 2590162

> AVP: l=6 t=Acct-Interim-Interval(85): 60

▼ AVP: l=24 t=Vendor-Specific(26) v=MikroTik(14988)

AVP Type: 26

AVP Length: 24

> VSA: l=18 t=Mikrotik-Rate-Limit(8): 1048576/10485760

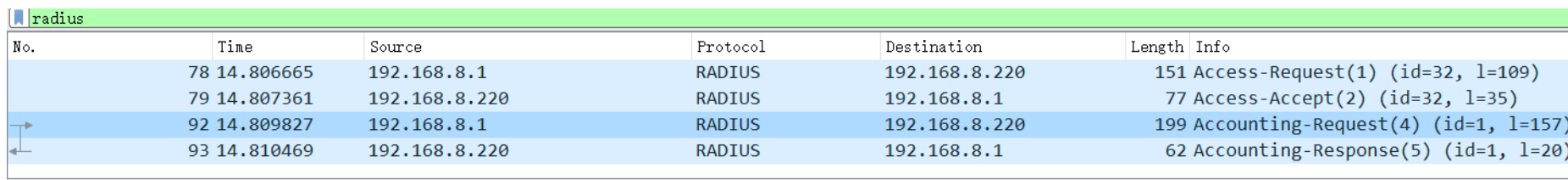
> AVP: l=12 t=Vendor-Specific(26) v=Roaring Penguin Software Inc.(10055)

> AVP: l=12 t=Vendor-Specific(26) v=Roaring Penguin Software Inc.(10055)



RADIUS计费报文(Accounting)

- 1) acc-status-type, 表示计费状态, start/update/stop;
- 2) user-name, 计费账号;
- 3) acc-session-id, 会话ID;
- 4) framed-ip-address, 用户IP;



Length: 157

Authenticator: 7315756964a4e15f7e399ab2d2f65fd3

[The response to this request is in frame 93]

- Attribute Value Pairs

- ```
> AVP: l=6 t=Service-Type(6): Framed(2)
> AVP: l=6 t=Framed-Protocol(7): PPP(1)
> AVP: l=6 t=NAS-Port(5): 6
> AVP: l=6 t=Acct-Status-Type(40): Start(1)
> AVP: l=6 t=Event-Timestamp(55): Apr 24, 2018 14:43:14.000000000
> AVP: l=19 t=Acct-Session-Id(44): PA_00031_e42ce0a7
> AVP: l=6 t=Acct-Session-Time(46): 0
> AVP: l=5 t=User-Name(1): lu0
> AVP: l=19 t=Calling-Station-Id(31): 54:e1:ad:20:7f:b8
> AVP: l=7 t=Called-Station-Id(30): PPP0E
> AVP: l=6 t=NAS-IP-Address(4): 192.168.8.1
> AVP: l=9 t=NAS-Identifier(32): Panabit
> AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
> AVP: l=6 t=Framed-IP-Address(8): 10.1.1.3
> AVP: l=6 t=Acct-Input-Octets(42): 0
> AVP: l=6 t=Acct-Input-Gigawords(52): 0
> AVP: l=6 t=Acct-Output-Octets(43): 0
> AVP: l=6 t=Acct-Output-Gigawords(53): 0
```



学校，学生，运营商三方共赢的方案

- 学生，可以自由选择运营商。
- 运营商，通过手机和宽带的绑定，可以增加自己用户数。
- 学校，学生网交给运营商维护，同时也能够解决对学生上网监管的问题。

**创建线路：**每次全新的PPPOE代拨，实际上是产生一条特定的“WAN线路”；

**IP和线路捆绑：**PPPOE代拨就是让内网指定的IP走这条特定的WAN线路出去，可以看着是将内网IP和WAN线路绑定的过程，简单说就是让IP走代拨的专线出去；

所有一切都是围绕上面两个原则设计的。

仅仅让内网IP走代拨线路NAT出去还不够，还要处理DNS请求。因为用户的IP是网内分配的，用户肯定有自己的DNS服务器，假如这个DNS是联通的，但是代拨线路是电信的，使用联通DNS解析出来的肯定是联通的IP了，从电信线路访问联通IP，那肯定是要出问题的。所以PPPOE代拨要有类似于DNS重定向的功能。



# 代拨设置



专业版

参数设置 在线用户

PPPOE代拨服务

不启用

默认网卡

em0

默认VLAN

0

默认MTU

1480

TTL

60

系统概况

当前策略

对象管理

账号管理

临时账号

RADIUS

文件类型

域名群组

IP群组

IP/MAC备注

应用路由

流量管理

其它管控

用户认证

应用识别

系统维护

组织架构 本地账号 代理账号

添加 用户组

上级节点

-

名称

地址范围

0.0.0.0 - 0.0.0.0

带宽限制

0 / 0 kbps,0表示不限制

DNS

0.0.0.0 例: 114.114.114.114,8.8.8.8

在线时间

0 小时,在线时间超过时,系统会主动踢用户下线,0表示不控制

过期用户

不能登陆

代拨设置

代拨主线

em0

主线VLAN

格式: 10或10/20

代拨副线

不设置

副线VLAN

格式: 10或10/20

代拨服务名

代拨时使用的PPPOE服务名称

帐号并发

0

代拨帐号最大并发IP数,0表示不限制

拨号次数

0

首次拨号失败后重拨次数,0表示不限制

确定

取消



# 策略路由



## 策略路由

| 序号    | 当前   | 源接口 | VLAN | TTL | 源地址/端口 | 目标地址/端口        | 协议  | 应用  | DSCP | 用户类型 | 动作   | 目标线路   | 下一跳 | 匹配次数 | 备注       | 添加策略                                                  |
|-------|------|-----|------|-----|--------|----------------|-----|-----|------|------|------|--------|-----|------|----------|-------------------------------------------------------|
| 90    | 任意时间 | any |      |     | any    | 172.168.0.138  | any | any |      | any  | NAT  | 缓存     |     | 0    |          | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 100   | 任意时间 | any |      |     | any    | 192.168.1.0/24 | any | any |      | any  | 路由   | 研发部1段  |     | 0    |          | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 110   | 任意时间 | any |      |     | any    | 192.168.0.1/24 | any | any |      | any  | 路由   | 研发部0段  |     | 4    |          | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 120   | 任意时间 | any |      |     | any    | 192.168.2.0/24 | any | any |      | any  | 路由   | 市场销售部  |     | 1    |          | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 130   | 任意时间 | any |      |     | any    | 192.168.8.0/24 | any | any |      | any  | 路由   | 技术部    |     | 2    |          | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 140   | 任意时间 | any |      |     | any    | 10.10.10.7     | any | any |      | any  | 路由   | PA访客网络 |     | 0    | AP管理IP地址 | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 800   | 任意时间 | any |      |     | any    | any            | any | any |      | any  | NAT  | 电信静态   |     | 58   |          | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 65500 | 任意时间 | any |      |     | any    | 60.60.60.60:80 | any | any |      | any  | 路由   | 电信静态   |     | 0    |          | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 65501 | 任意时间 | any |      |     | any    | any            | any | any |      | 代拨   | 走代拨线 | 代拨线路   |     | 0    | 代拨路由     | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |

## 专业版

## 策略管理 QPS趋势

| 序号  | 路径  | 源接口 | VLAN | 源地址 | 目标地址 | 访问域名 | 应用协议 | 用户类型 | 执行动作                   | 单IP-QPS | 匹配后 | 动作前/后QPS | 丢弃/命中 | 添加策略>                                                 |
|-----|-----|-----|------|-----|------|------|------|------|------------------------|---------|-----|----------|-------|-------------------------------------------------------|
| 400 | any | any |      | any | any  | test | any  | any  | 解析为IP->220.181.111.188 | 0       | 停止  | 0/0      | 0/0   | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 500 | any | any |      | any | any  | any  | any  | any  | 牵引至->电信静态              | 0       | 停止  | 7/7      | 0/530 | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |
| 600 | any | any |      | any | any  | any  | any  | 代拨   | 代拨重定向                  | 0       | 停止  | 0/0      | 0/0   | <a href="#">✎</a> <a href="#">✕</a> <a href="#">⏸</a> |

计费向 Panabit 发送 COA (code=0x2b) 数据包, COA 数据包中包含如下属性:

- 1) User-Name (0x01) : 代拨帐号名称; 【必须】
- 2) User-Password (0x02) : 代拨帐号密码, 需要注意的是, RADIUS 规范里 User-Password 是加密的, 但是 Panabit 要求这里的 User-Password 不能加密; 【必须】
- 3) Filter-Id (0x0b) : 这个属性的值为 “\_PAIPXY\_”, 这个值表示这是一个需要 Panabit 执行代拨的 COA 指令; 【必须】
- 4) Framed-IP-Address (0x08) : 这个属性里存储的是要捆绑的内网 IP 地址; 【必须】
- 5) Framed-Pool (0x58) : 存放的是地址池名称, Panabit 会根据这个地址池名称来 寻找外拨接口和 VLAN 参数, 地址池需要事先在 Panabit 上设置好, 如果没有这个属性, Panabit 使用代拨模块默认配置的代拨信息拨号; 【可选】
- 6) Connect-Info(0x4d): 这个参数里存储的是内网用户帐号名称, 如果没有这个属性, Panabit 使用 User-Name 作为内网 IP 的账号名称; 【可选】
- 7) Port-Id(0x57) : 这个参数里存储的是代拨帐号对应的 VLAN 信息, 格式为 “10/20 “或” 10 “, 其中 10 为外层 VLAN, 20 为内层 VLAN; 这个参数优先于 Framed-Pool 指向的地址池对象里设置的 VLAN 参数; 【可选】
- 8) Called-Station-Id (0x1e) or Calling-Station-Id (0x1f) : 这个参数的格式为 “xx:xx:xx:xx:xx:xx” 或 “xx-xx-xx-xx-xx-xx”, 存放要捆绑的 IP 的 MAC 地址, 这个 MAC 地址只是描述作用, 如果计费和用户之间有三层交换机不能获取到真实的 MAC 地址, 也可以用三层交换的 MAC;

Panabit 收到 COA 请求后:

- 1) 如果成功拨号, 返回 COA ACK (0x2c) ;
- 2) 如果拨号失败, 返回 COA NAK(0x2d), 失败的原因会放到 Reply-Message 属性里, 这个属性是一个字符串; 如果是认证错误, Panabit 会将 BRAS 返回的错误信息放在 Reply-Message 里传递给 AAA;

常见的 Reply-Message 值:

- 1) " POOLNEXIST" :指定了 Framed-Pool 属性, 但是该属性指定的地址池在 Panabit 上没有找到;
- 2) "IPOBJ\_INSTALL\_FAIL" : 创建内网 IP 对象失败, 可能是授权不够, 也可能是指定的 IP 不在合法 IP 范围内;
- 3) "IPOVERFLOW" : 代拨账号关联的内网 IP 数超过设定的最大值;
- 4) "IPPTY\_NOOUTINTERFACE" : 没有指定代拨外出网口;
- 5) 其它信息: 拨号认证失败后, BRAS 返回的信息;

| radius |          |               |          |               |        |                                               |
|--------|----------|---------------|----------|---------------|--------|-----------------------------------------------|
| No.    | Time     | Source        | Protocol | Destination   | Length | Info                                          |
| → 210  | 3.314934 | 192.168.8.115 | RADIUS   | 192.168.8.122 | 122    | CoA-Request(43) (id=54, l=80)                 |
| ← 218  | 3.356339 | 192.168.8.122 | RADIUS   | 192.168.8.115 | 74     | CoA-ACK(44) (id=54, l=32)                     |
| ← 225  | 3.369774 | 192.168.8.122 | RADIUS   | 192.168.8.115 | 74     | CoA-ACK(44) (id=54, l=32), Duplicate Response |

> Frame 210: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0

> Ethernet II, Src: AsustekC\_10:0d:06 (d0:17:c2:10:0d:06), Dst: b0:7d:99:1b:00:00 (b0:7d:99:1b:00:00)

> Internet Protocol Version 4, Src: 192.168.8.115, Dst: 192.168.8.122

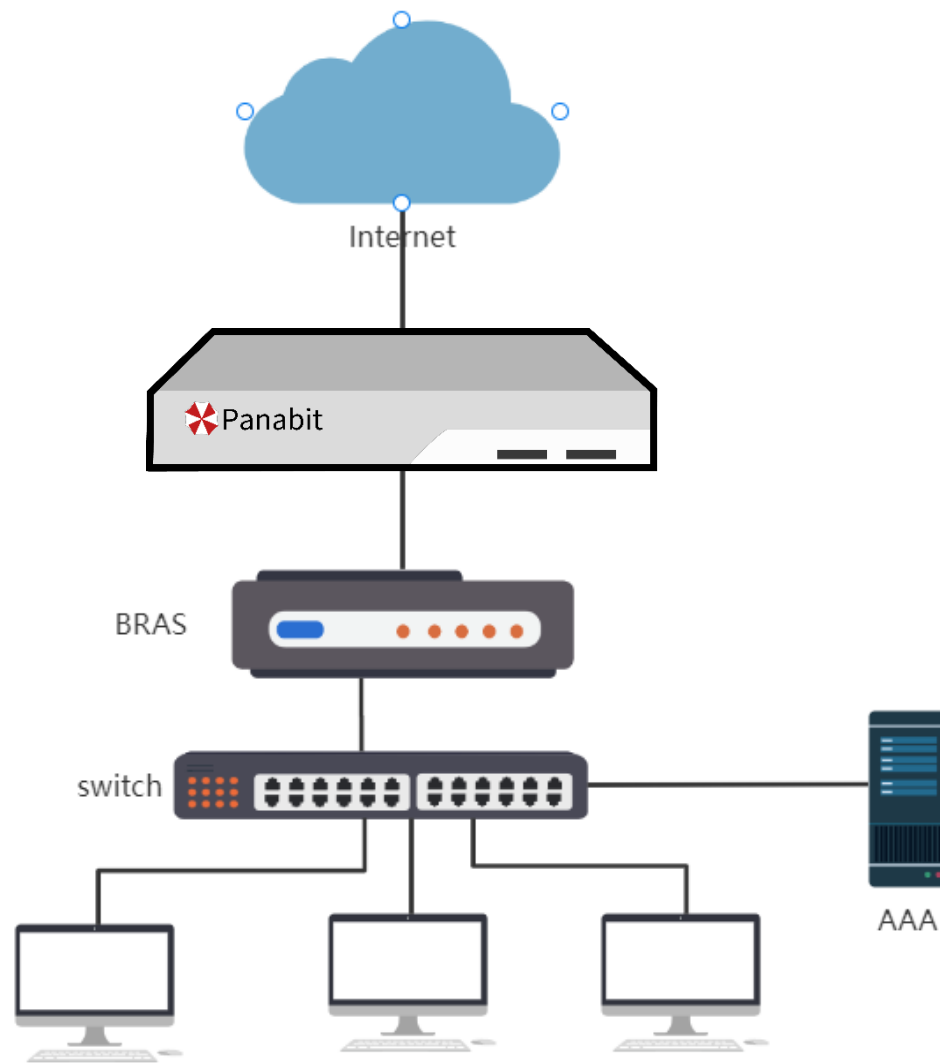
> User Datagram Protocol, Src Port: 50347, Dst Port: 3799

▼ RADIUS Protocol

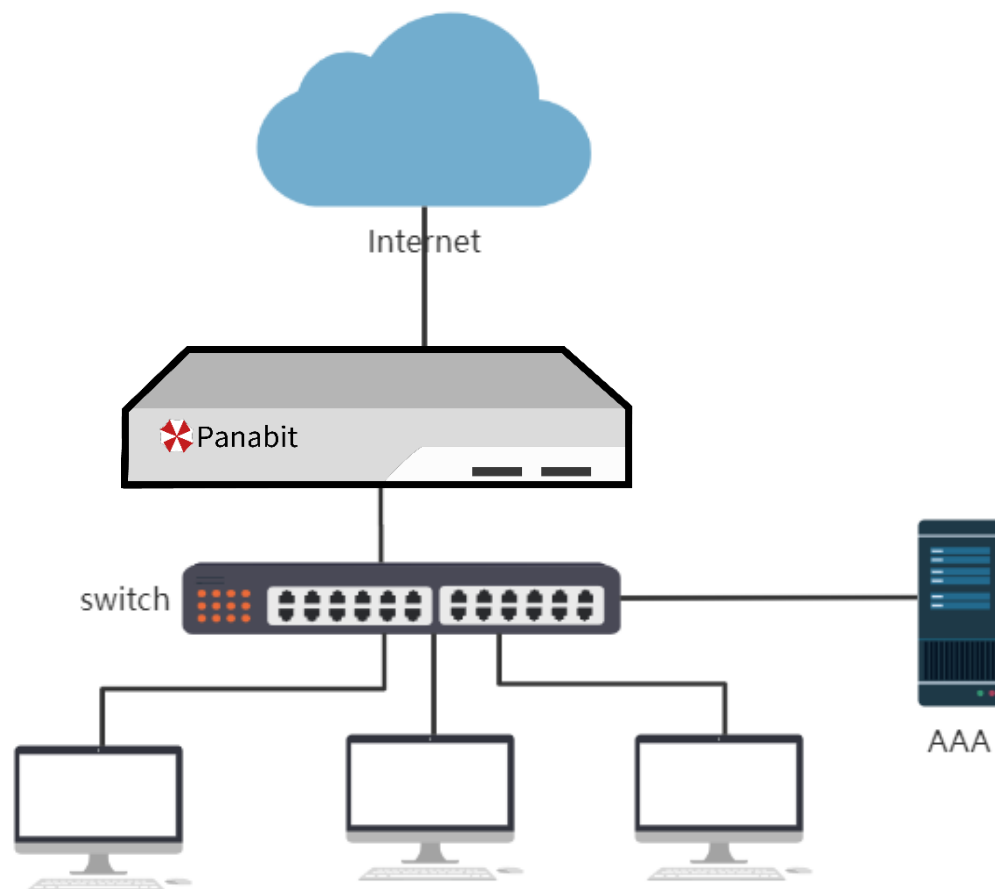
Code: CoA-Request (43)  
Packet identifier: 0x36 (54)  
Length: 80  
Authenticator: 1f37d6435dfef966400b8960275944ad  
[\[The response to this request is in frame 218\]](#)

▼ Attribute Value Pairs

> AVP: l=5 t=User-Name(1): zrk  
> AVP: l=5 t=User-Password(2): Encrypted  
> AVP: l=6 t=Framed-IP-Address(8): 10.10.100.11  
> AVP: l=13 t=Filter-Id(11): \_\_PAIPXY\_\_  
> AVP: l=7 t=NAS-Port-Id(87): 10/20  
> AVP: l=5 t=Framed-Pool(88): AAA  
> AVP: l=19 t=Called-Station-Id(30): F8-CF-C5-83-09-B9









**THANK YOU**