认证培训

认证的目的

1）差异化管理

2）计费

3）实名审计

关键词

■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。

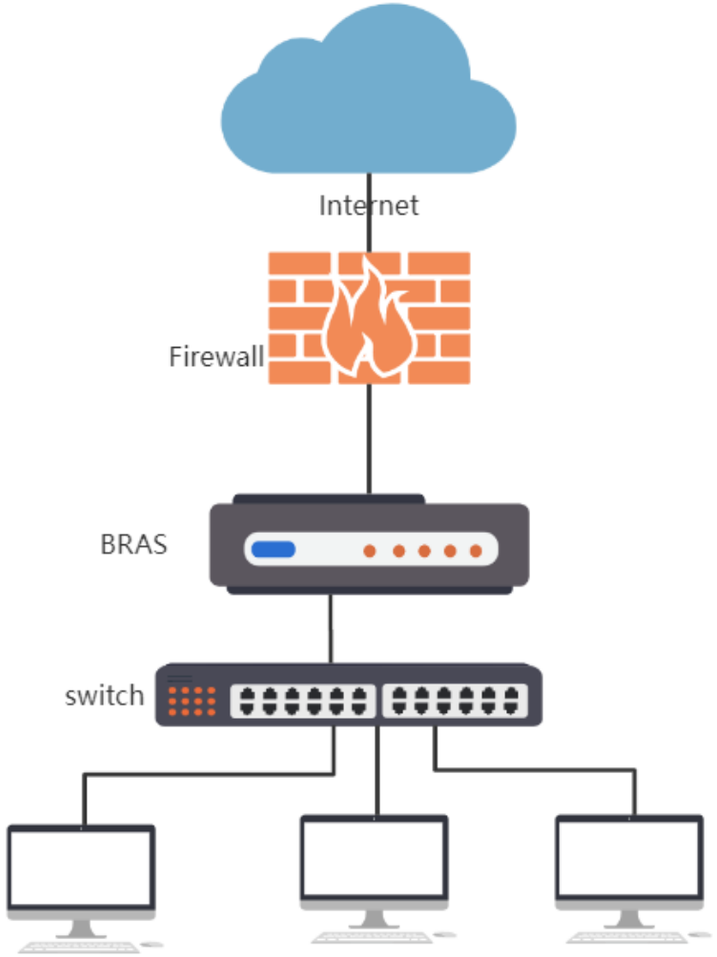
■cmccportal

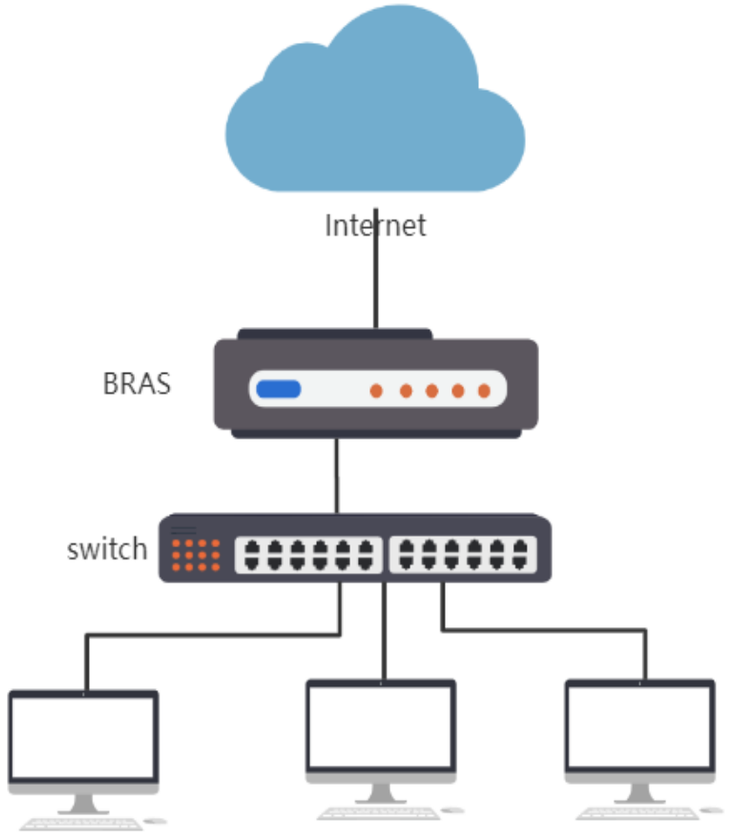
认证方式

■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

部署方式





Portal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

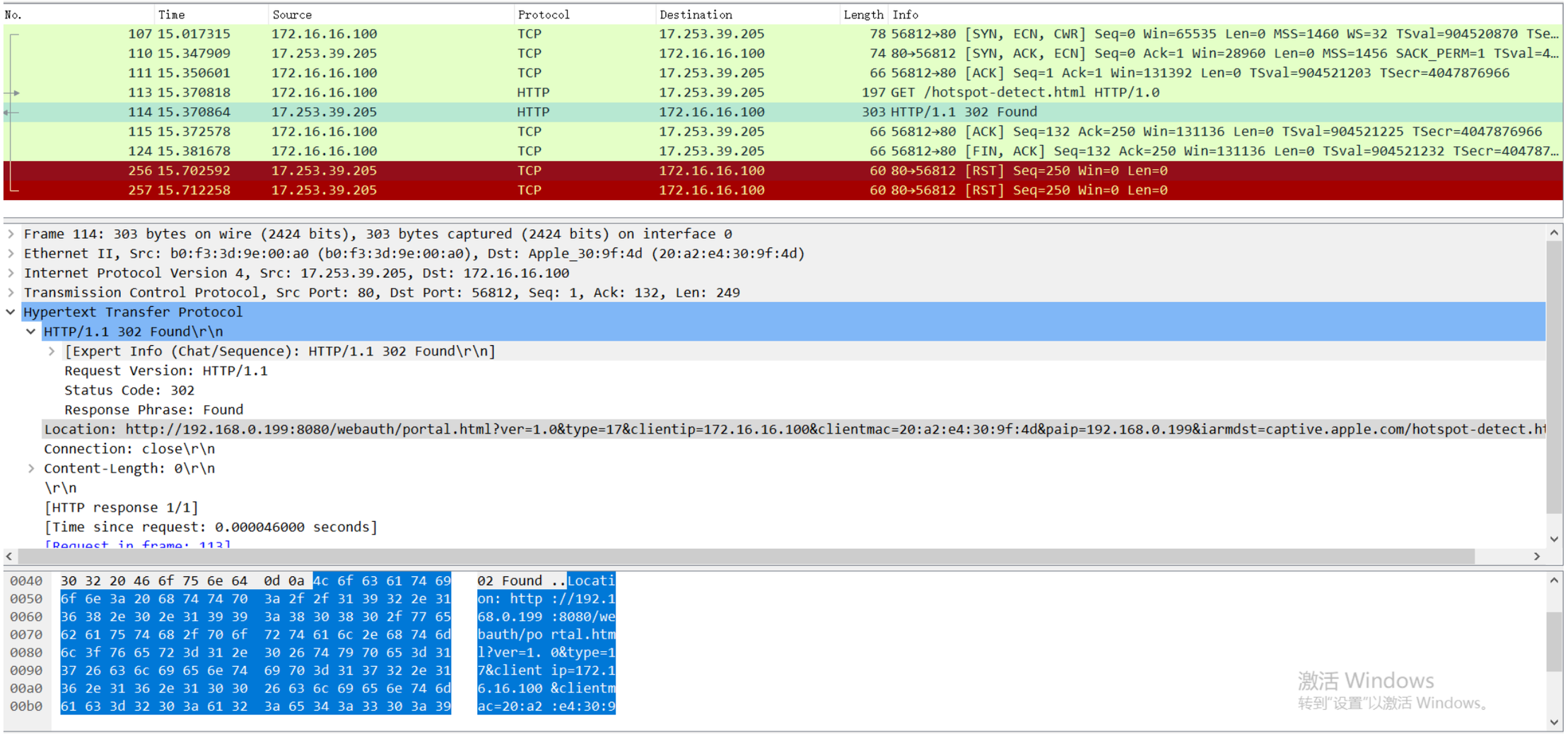
Portal认证-关键技术

■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；换而言之，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

Panabit®



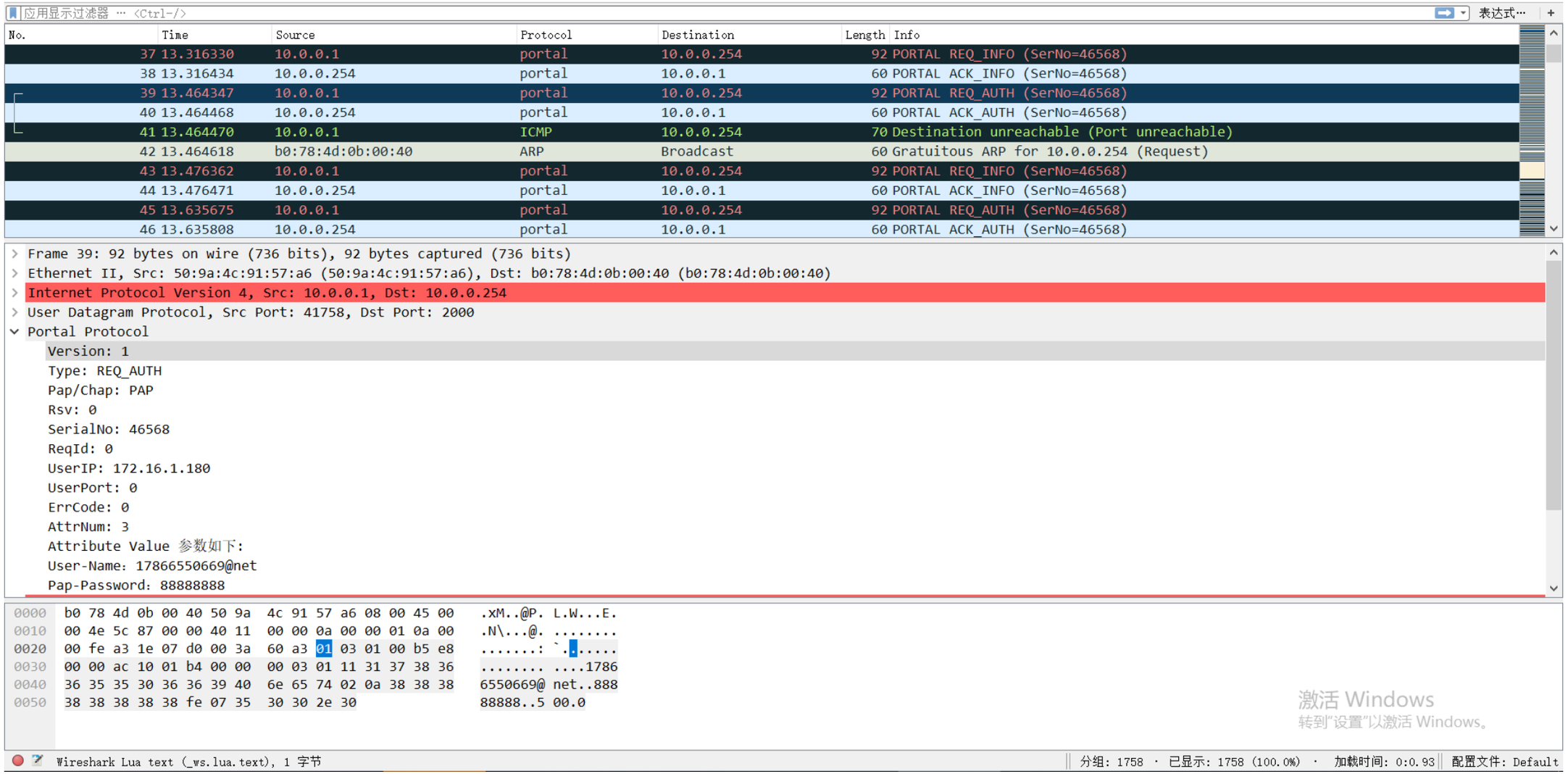
No.	Time	Source	Protocol	Destination	Length	Info
107	15.017315	172.16.16.100	TCP	17.253.39.205	78	56812→80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=904520870 TSe…
110	15.347909	17.253.39.205	TCP	172.16.16.100	74	80→56812 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1456 SACK_PERM=1 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.ht
    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
```

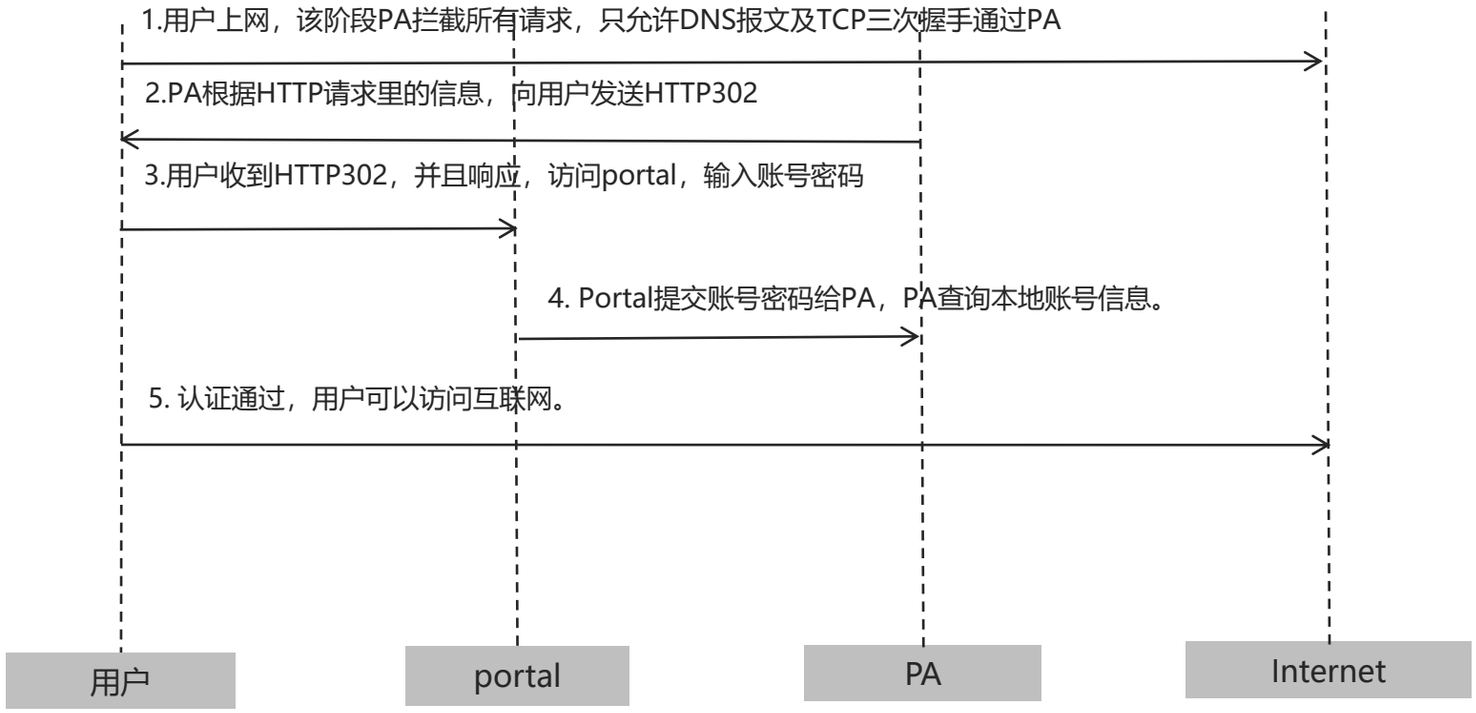
cmccportal

Panabit®

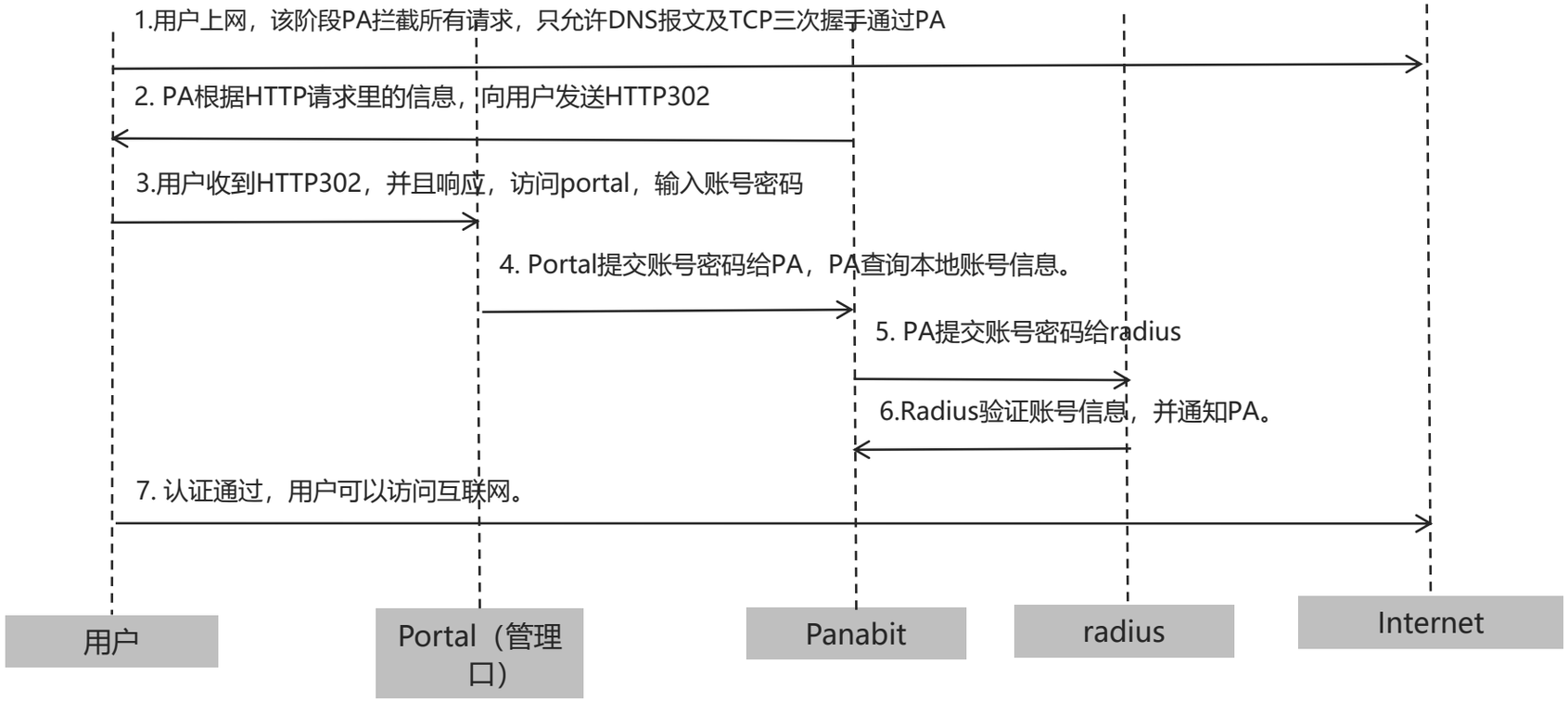


WEB认证配置

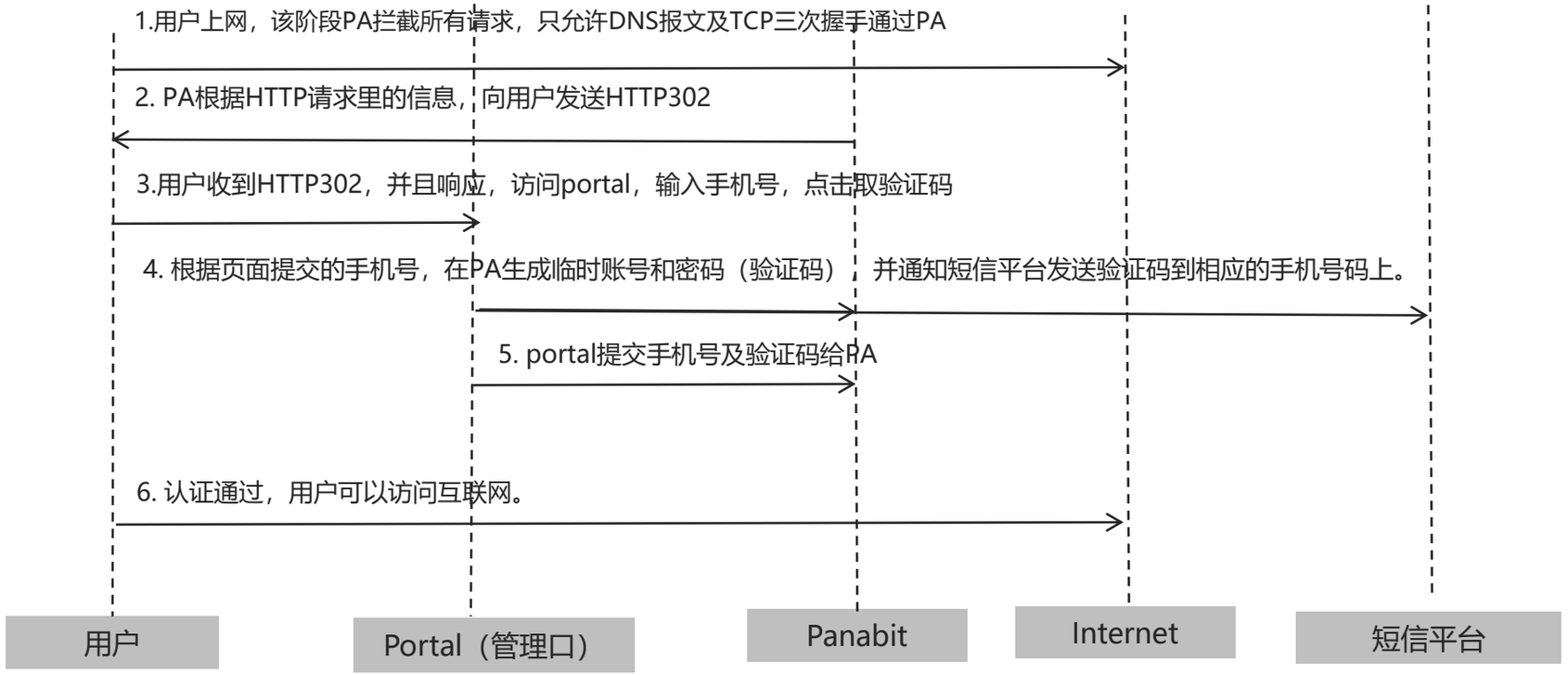
本地认证



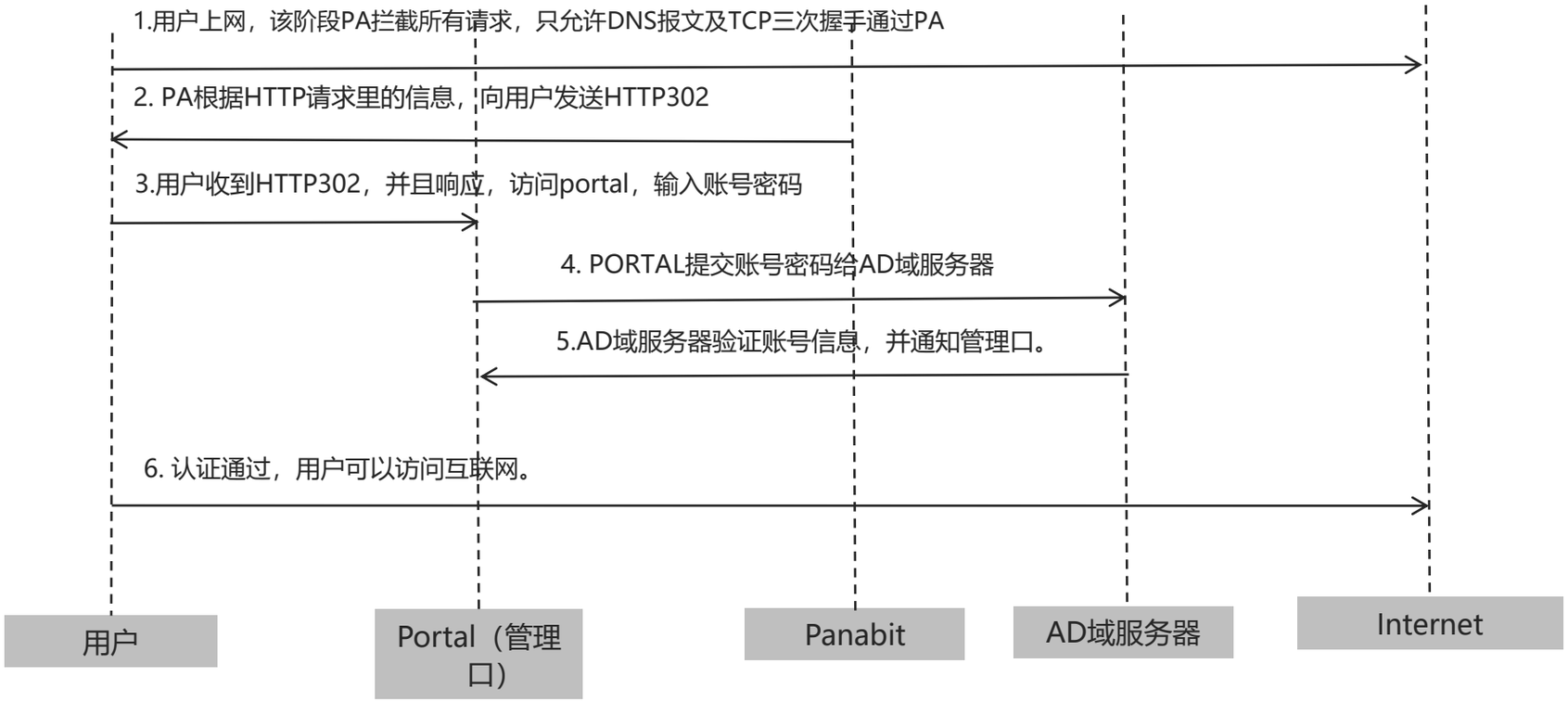
radius认证



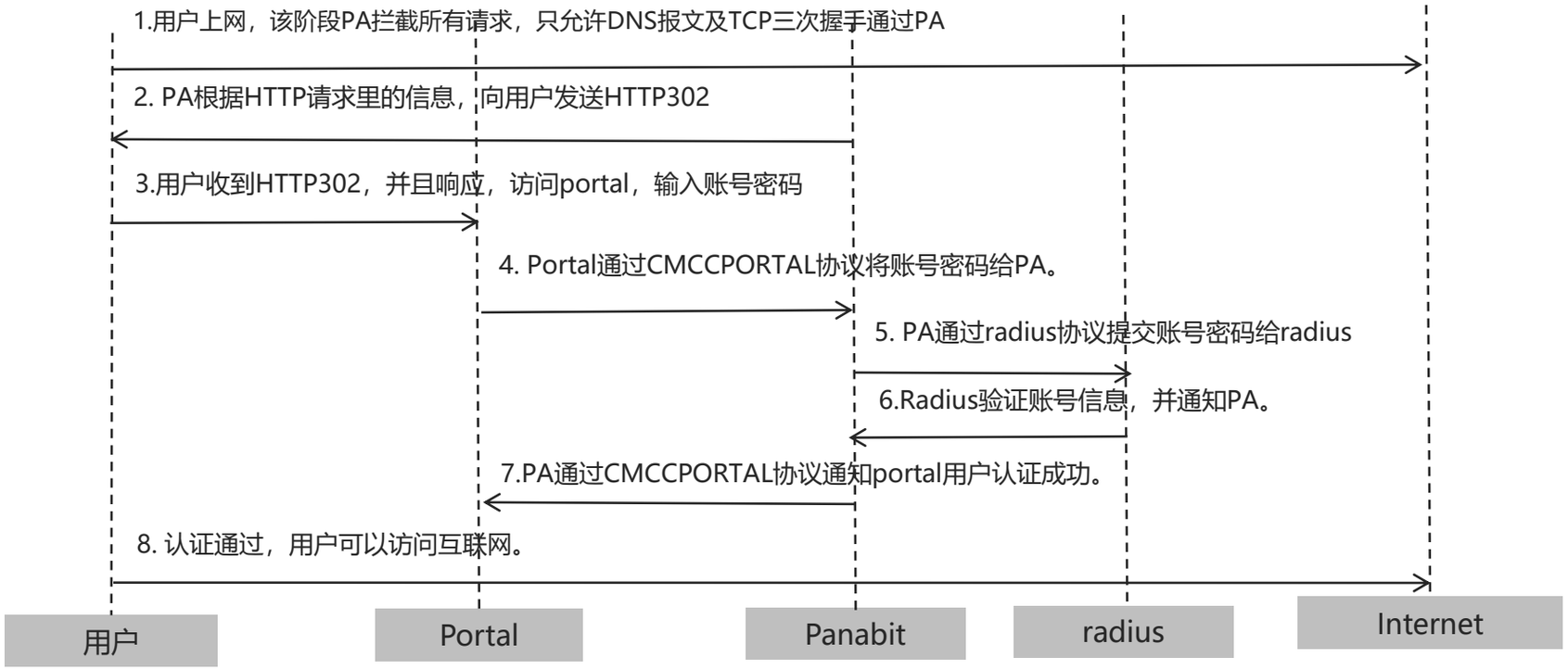
短信认证



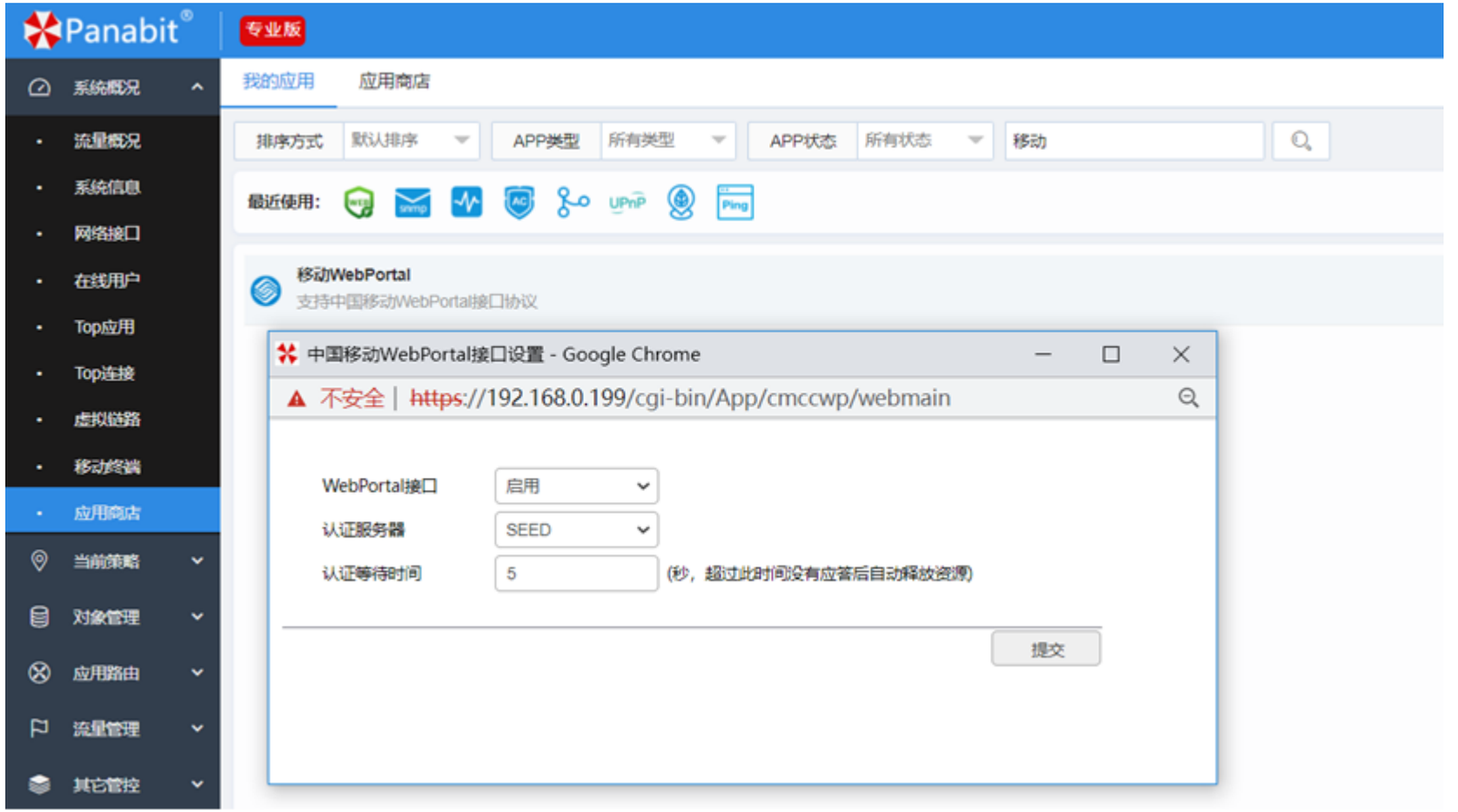
AD域认证



第三方portal认证



第三方portal认证

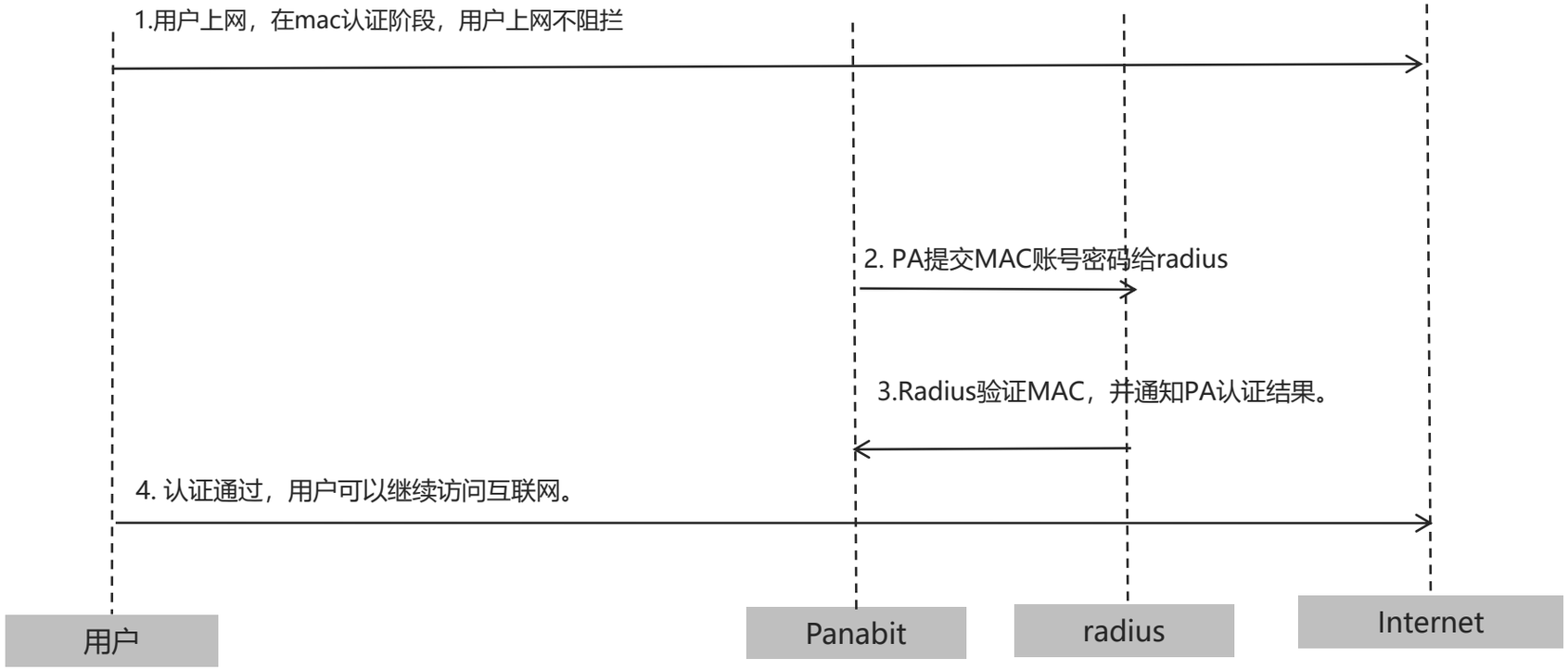


MAC无感知认证

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

MAC无感知认证流程



跨三层MAC获取

■跨三层取MAC

■DHCPSINF

命令行输入

floweye dhcpsnif4 config enable=1

PPPOE认证

■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认证

■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

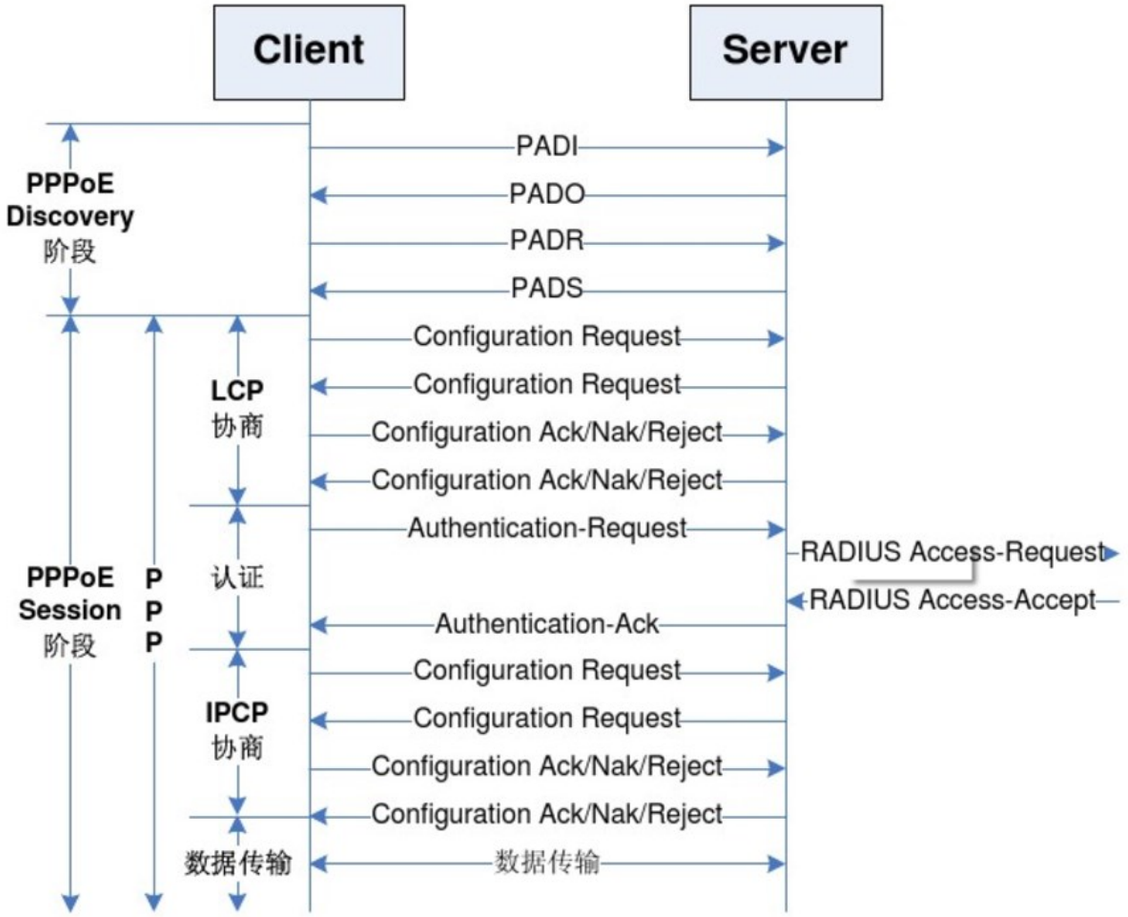
--需要客户端支持

--必须是二层网络架构

PPPOE

- PPPoE分成两个阶段：

1. PPPoE发现阶段；
2. PPPoE会话阶段。



discovery

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

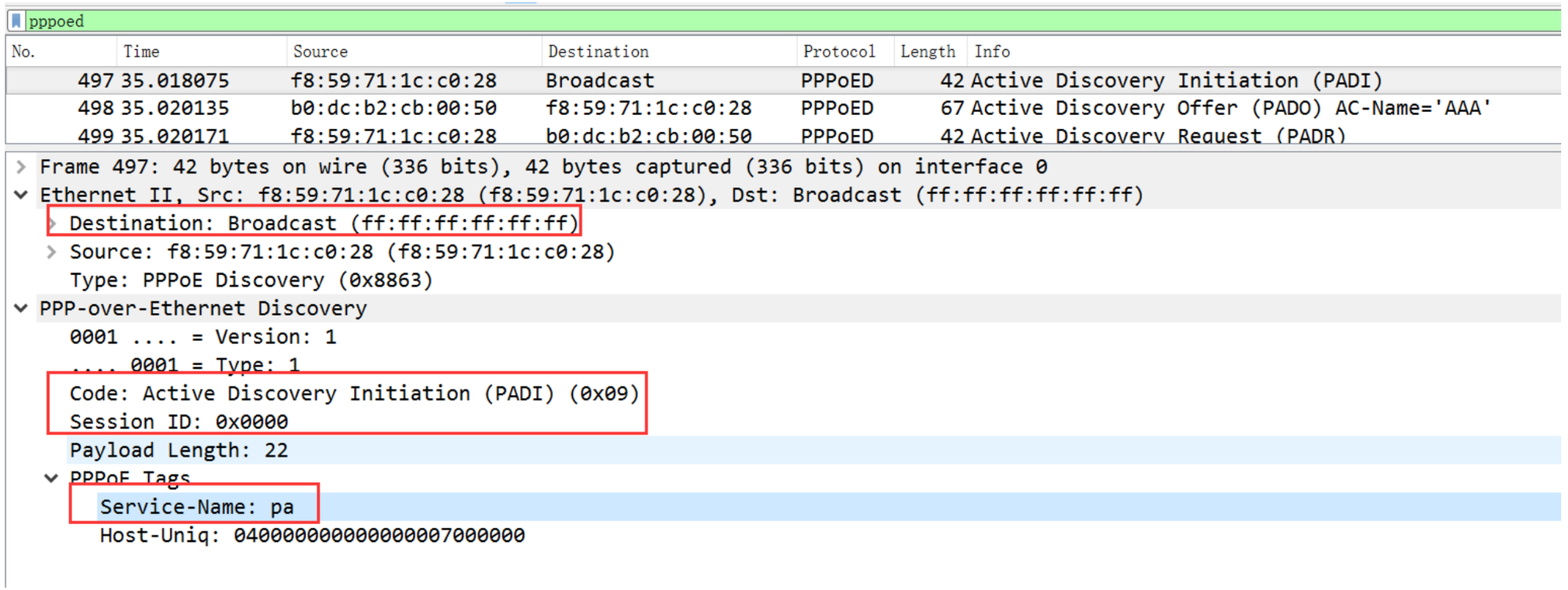
◆client发送单播**SessionRequest**(PADR)数据包

◆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?

PADI



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

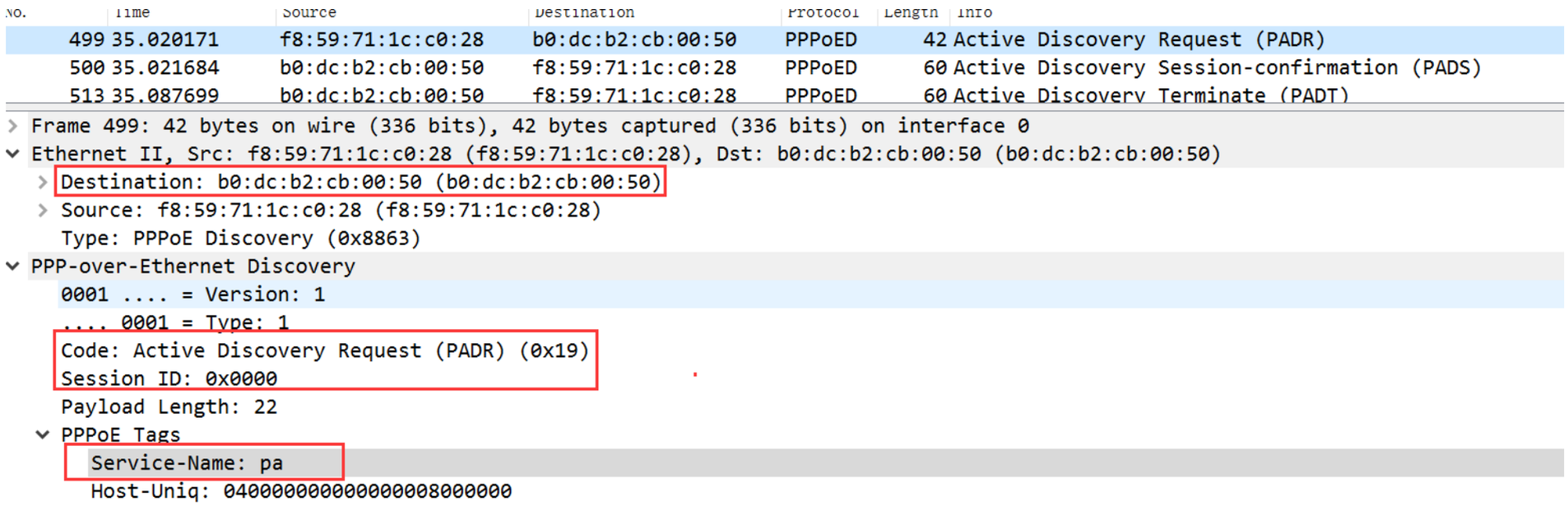
PADO

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
v 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)
v PPP-over-Ethernet Discovery
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Active Discovery Offer (PADO) (0x07)
    Session ID: 0x0000
    Payload Length: 29
  v PPPoE Tags
      Service-Name: pa
      Host-Uniq: 0400000000000000007000000
      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）

PADR



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

PADS

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
v 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)
v PPP-over-Ethernet Discovery
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Active Discovery Session-confirmation (PADS) (0x65)
    Session ID: 0x0002
    Payload Length: 22
  v 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；

PPP的四个阶段

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；

PPP阶段的特性

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
v Point-to-Point Protocol
    Protocol: Internet Protocol Control Protocol (0x8021)
v PPP IP Control Protocol
    Code: Configuration Request (1)
    Identifier: 6 (0x06)
    Length: 34
  v 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
v Point-to-Point Protocol
    Protocol: Internet Protocol Control Protocol (0x8021)
v PPP IP Control Protocol
    Code: Configuration Reject (4)
    Identifier: 6 (0x06)
    Length: 16
  v 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

IPCP Request数据包截图

```
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。

IPCP NAK数据包截图数据包截图

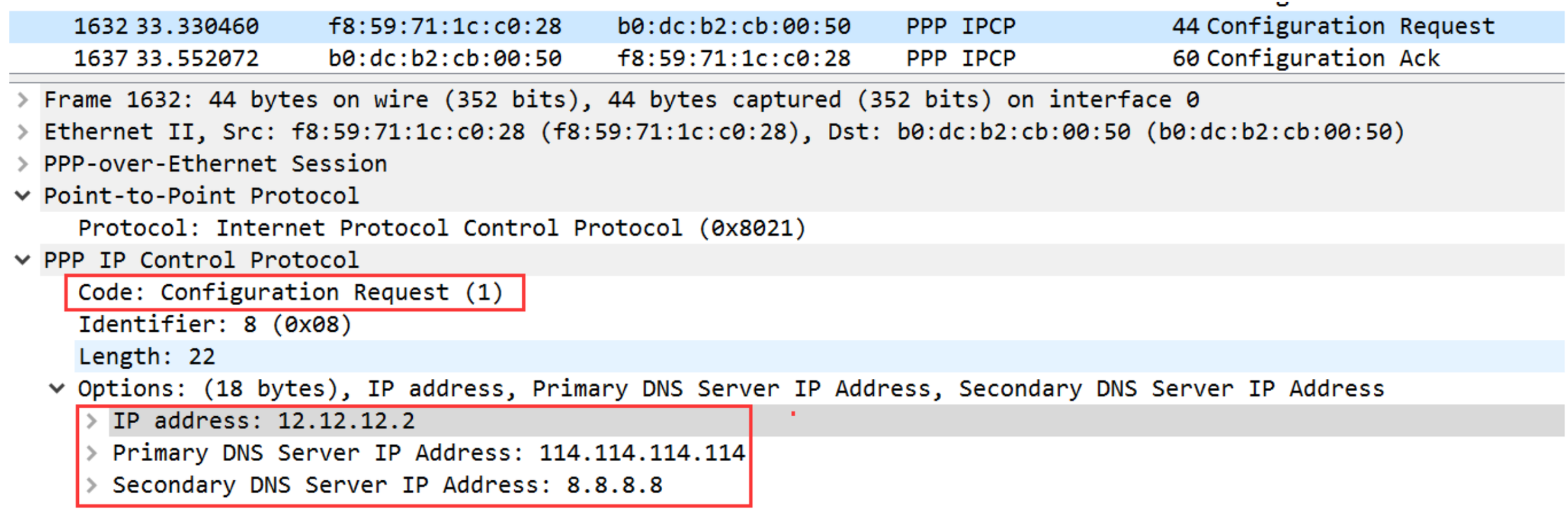
Panabit®

```
   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
v Point-to-Point Protocol
    Protocol: Internet Protocol Control Protocol (0x8021)
v PPP IP Control Protocol
    Code: Configuration Nak (3)
    Identifier: 7 (0x07)
    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。

IPCP Request数据包截图



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

IPCP ACK数据包截图

```
    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。

PPPoE （PADT）

```
    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)
v 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。

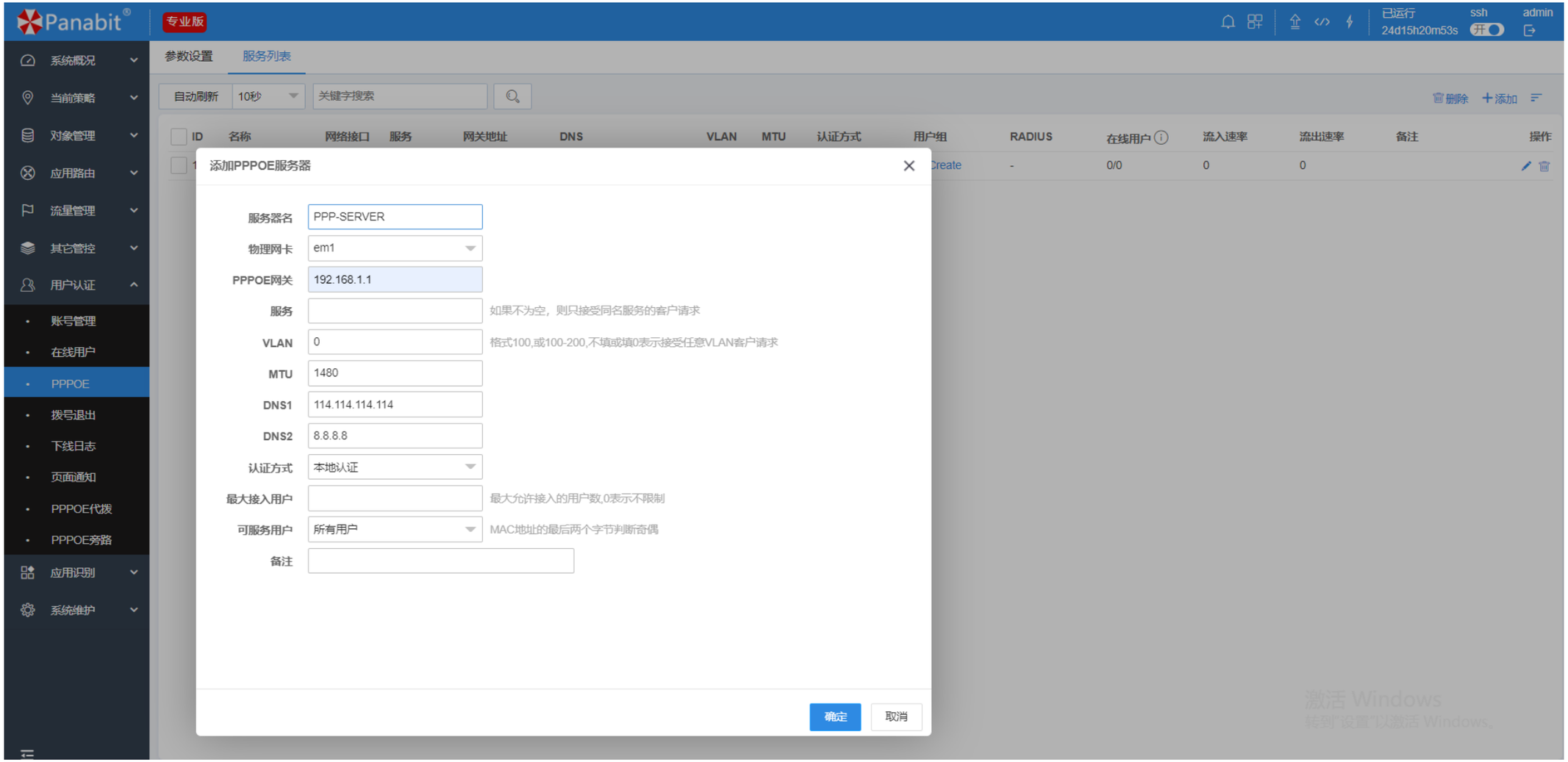
其它事项

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

PPPOE



PPPOE认证方式

■本地认证

■radius认证

■先本地后radius认证

■免认证

PPPOE的另类认证

■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
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x20 (32)
    Length: 109
    Authenticator: 4d830000e175ac21b2596f410aa81f97
    [The response to this request is in frame 79]
  v Attribute Value Pairs
    > AVP: l=5 t=User-Name(1): luo
    > 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): PPPOE
    > 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
```

Panabit 如何分配IP地址给客户

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

Access-Accpet

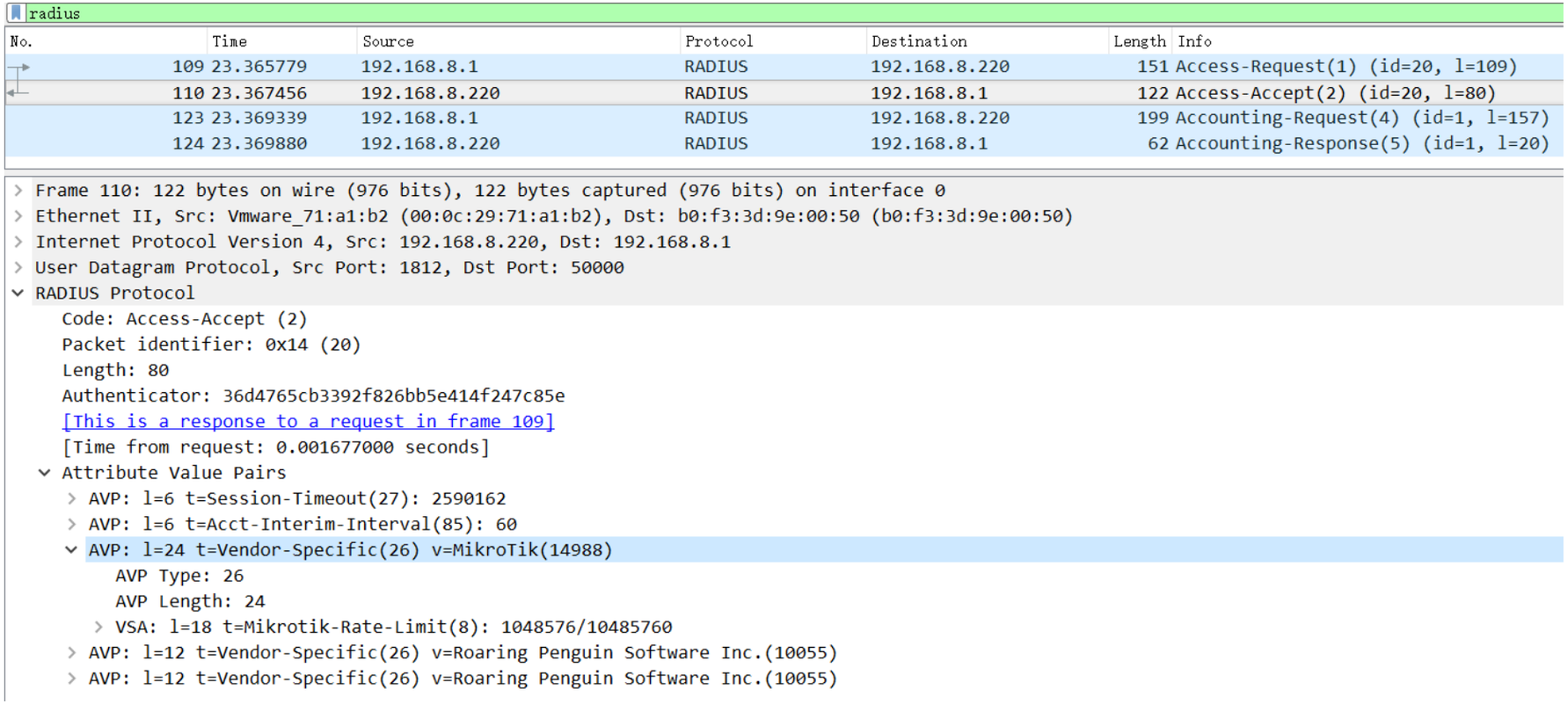
Panabit®

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
v 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]
  v 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
```

Access-Accpet



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；

RADIUS计费(Accounting)

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)

```
Packet identifier: 0x1 (1)
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 ��й������ʱ��
  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): luo
  AVP: l=19 t=Calling-Station-Id(31): 54:e1:ad:20:7f:b8
  AVP: l=7 t=Called-Station-Id(30): PPPOE
  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
```

代拨

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。

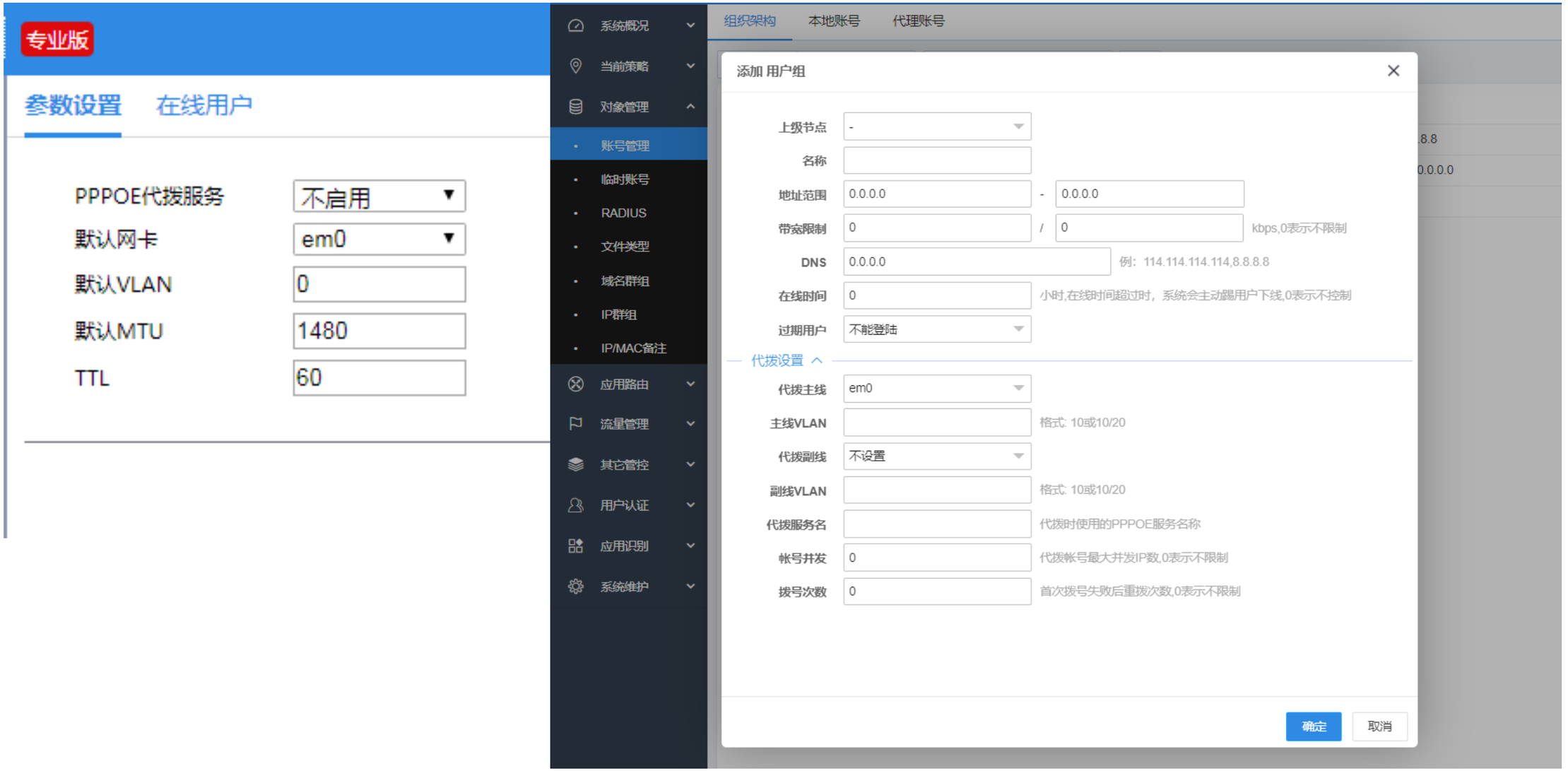
正确理解代拨

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



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		
100	任意时间	any			any	192.168.1.0/24	any	any		any	路由	研发部1段		0		
110	任意时间	any			any	192.168.0.1/24	any	any		any	路由	研发部0段		4		
120	任意时间	any			any	192.168.2.0/24	any	any		any	路由	市场销售部		1		
130	任意时间	any			any	192.168.8.0/24	any	any		any	路由	技术部		2		
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	
800	任意时间	any			any	any	any	any		any	NAT	电信静态		58		
65500	任意时间	any			any	60.60.60.60:80	any	any		any	路由	电信静态		0		
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	

专业版 已运行 2d23h26m52s SSH admin

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	
500	any	any		any	any	any	any	any	牵引至->电信静态	0	停止	7/7	0/530	
600	any	any		any	any	any	any	代拨	代拨重定向	0	停止	0/0	0/0	

代拨接口

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“__PAIPPXY__“，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；

代拨

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） “IPPXY_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；

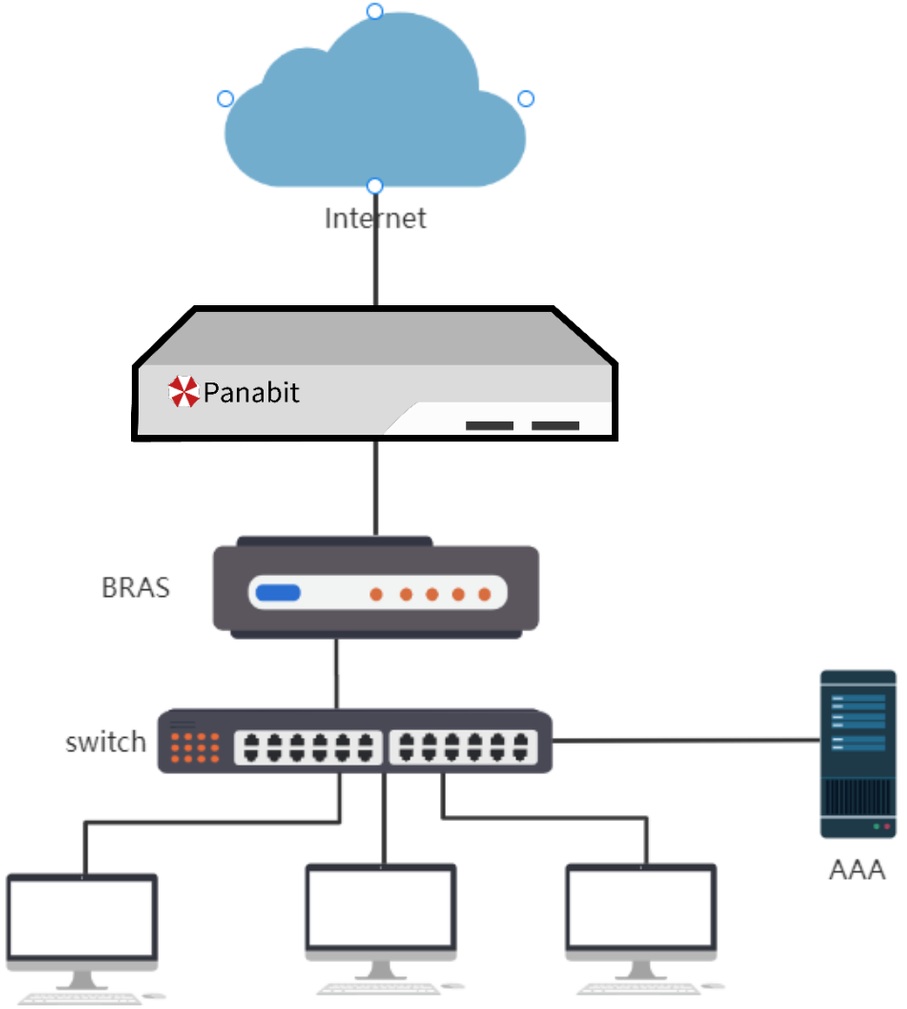
代拨报文

radius

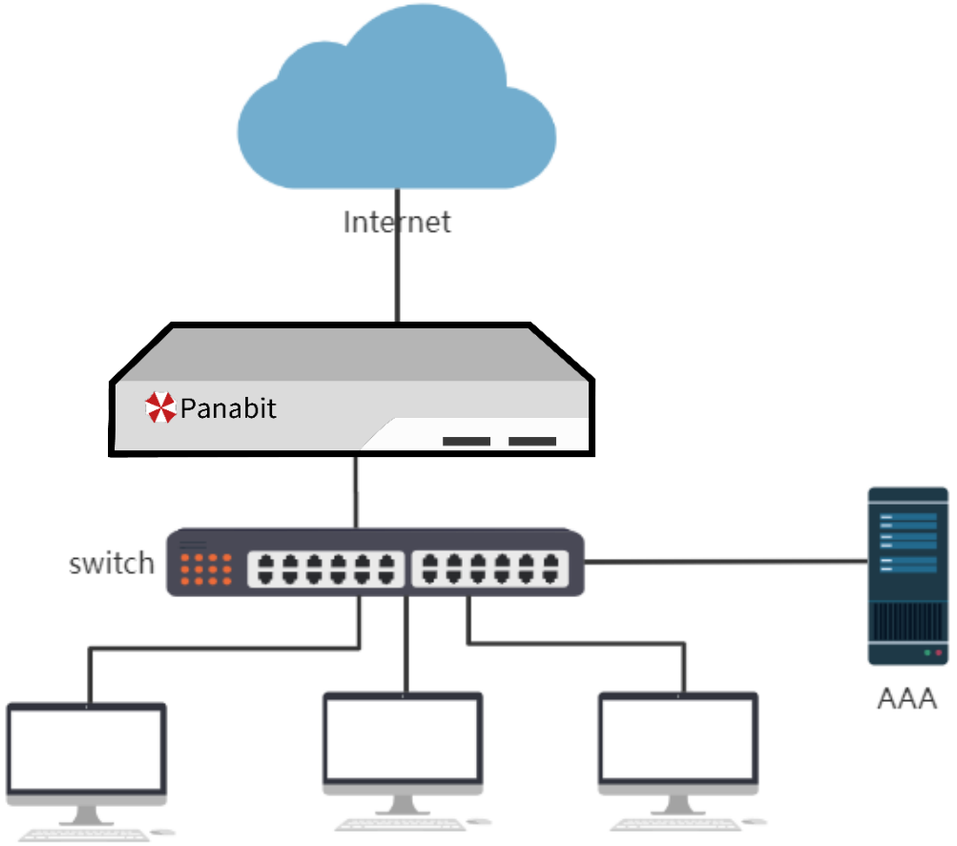
No.	Time	Source	Protocol	Destination	Length	Info
210	3.314934	192.168.8.115	RADIUS	192.168.8.122	122	CoA-Request(43) (id=54, l=80)
218	3.356339	192.168.8.122	RADIUS	192.168.8.115	74	CoA-ACK(44) (id=54, l=32)
225	3.369774	192.168.8.122	RADIUS	192.168.8.115	74	CoA-ACK(44) (id=54, l=32), Duplicate Response

```
> 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
v RADIUS Protocol
    Code: CoA-Request (43)
    Packet identifier: 0x36 (54)
    Length: 80
    Authenticator: 1f37d6435dfeb966400b8960275944ad
    [The response to this request is in frame 218]
  v 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): __PAIPPXY__
    > 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
```

代拨拓扑



代拨拓扑



THANK YOU