目 录

1 PPP

1.1 PPP简介

PPP（Point-to-Point Protocol，点对点协议）是一种点对点的链路层协议。它能够提供用户认证，易于扩充，并且支持同/异步通信。

PPP 定义了一整套协议，包括：

- 链路控制协议（Link Control Protocol，LCP）：用来建立、拆除和监控数据链路。
- 网络控制协议（Network Control Protocol，NCP）：用来协商在数据链路上所传输的网络层报文的一些属性和类型。
- 认证协议：用来对用户进行认证，包括 PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）、MSCHAP（Microsoft CHAP，微软 CHAP 协议）和 MSCHAPv2（微软 CHAP 协议版本 2）。

1. PPP链路建立过程

PPP链路建立过程如 图 1-1 所示：

(1) PPP 初始状态为不活动（Dead）状态，当物理层 Up 后，PPP 会进入链路建立（Establish）阶段。

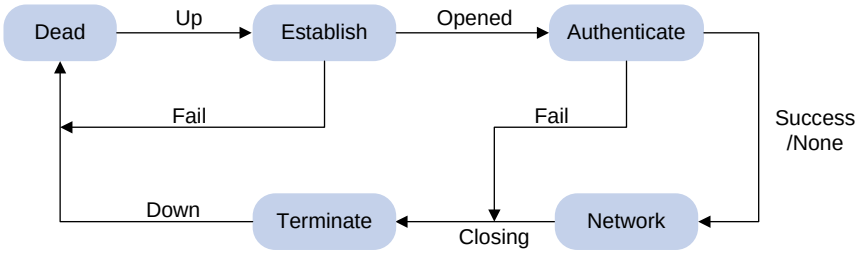
(2) PPP 在 Establish 阶段主要进行 LCP 协商。LCP 协商内容包括：Authentication-Protocol（认证协议类型）、ACCM（Async-Control-Character-Map，异步控制字符映射表）、MRU（Maximum-Receive-Unit，最大接收单元）、Magic-Number（魔术字）、PFC（Protocol-Field-Compression，协议字段压缩）、ACFC（Address-and-Control-Field-Compression，地址控制字段压缩）、MP 等选项。如果 LCP 协商失败，LCP 会上报 Fail 事件，PPP 回到 Dead 状态；如果 LCP 协商成功，LCP 进入 Opened 状态，LCP 会上报 Up 事件，表示链路已经建立（此时对于网络层而言 PPP 链路还没有建立，还不能够在上面成功传输网络层报文）。

(3) 如果配置了认证，则进入 Authenticate 阶段，开始 PAP、CHAP、MSCHAP 或 MSCHAPv2 认证。如果认证失败，LCP 会上报 Fail 事件，进入 Terminate 阶段，拆除链路，LCP 状态转为 Down，PPP 回到 Dead 状态；如果认证成功，LCP 会上报 Success 事件。

(4) 如果配置了网络层协议，则进入 Network 协商阶段，进行 NCP 协商（如 IPCP 协商、IPv6CP 协商）。如果 NCP 协商成功，链路就会 UP，就可以开始承载协商指定的网络层报文；如果 NCP 协商失败，NCP 会上报 Down 事件，进入 Terminate 阶段。（对于 IPCP 协商，如果接口配置了 IP 地址，则进行 IPCP 协商，IPCP 协商通过后，PPP 才可以承载 IP 报文。IPCP 协商内容包括：IP 地址、DNS 服务器地址等。）

(5) 到此，PPP 链路将一直保持通信，直至有明确的 LCP 或 NCP 消息关闭这条链路，或发生了某些外部事件（例如用户的干预）。

图1-1 PPP 链路建立过程



有关 PPP 的详细介绍请参考 RFC 1661。

2. PPP认证

PPP 提供了在其链路上进行安全认证的手段，使得在 PPP 链路上实施 AAA 变的切实可行。将 PPP 与 AAA 结合，可在 PPP 链路上对对端用户进行认证、计费。

PPP 支持如下认证方式：PAP、CHAP、MSCHAP、MSCHAPv2。

(1) PAP 认证

PAP 为两次握手协议，它通过用户名和密码来对用户进行认证。

PAP 在网络上以明文的方式传递用户名和密码，认证报文如果在传输过程中被截获，便有可能对网络安全造成威胁。因此，它适用于对网络安全要求相对较低的环境。

(2) CHAP 认证

CHAP 为三次握手协议。

CHAP 认证过程分为两种方式：认证方配置了用户名、认证方没有配置用户名。推荐使用认证方配置用户名的方式，这样被认证方可以对认证方的身份进行确认。

CHAP 只在网络上传输用户名，并不传输用户密码（准确的讲，它不直接传输用户密码，传输的是用 MD5 算法将用户密码与一个随机报文 ID 一起计算的结果），因此它的安全性要比 PAP 高。

(3) MSCHAP 认证

MSCHAP 为三次握手协议，认证过程与 CHAP 类似，MSCHAP 与 CHAP 的不同之处在于：

- MSCHAP 采用的加密算法是 0x80。
- MSCHAP 支持重传机制。在被认证方认证失败的情况下，如果认证方允许被认证方进行重传，被认证方会将认证相关信息重新发回认证方，认证方根据此信息重新对被认证方进行认证。认证方最多允许被认证方重传 3 次。

(4) MSCHAPv2 认证

MSCHAPv2 为三次握手协议，认证过程与 CHAP 类似，MSCHAPv2 与 CHAP 的不同之处在于：

- MSCHAPv2 采用的加密算法是 0x81。
- MSCHAPv2 通过报文捎带的方式实现了认证方和被认证方的双向认证。
- MSCHAPv2 支持重传机制。在被认证方认证失败的情况下，如果认证方允许被认证方进行重传，被认证方会将认证相关信息重新发回认证方，认证方根据此信息重新对被认证方进行认证。认证方最多允许被认证方重传 3 次。
- MSCHAPv2 支持修改密码机制。被认证方由于密码过期导致认证失败时，被认证方会将用户输入的新密码信息发回认证方，认证方根据新密码信息重新进行认证。

3. PPP支持IPv4

在 IPv4 网络中，PPP 进行 IPCP 协商过程中可以进行 IP 地址、DNS 服务器地址的协商。

(1) IP 地址协商

PPP 在进行 IPCP 协商的过程中可以进行 IP 地址的协商，即一端给另一端分配 IP 地址。

在 PPP 协商 IP 地址的过程中，设备可以分为两种角色：

- Client 端：若本端接口封装的链路层协议为 PPP 但还未配置 IP 地址，而对端已有 IP 地址时，用户可为本端接口配置 IP 地址可协商属性，使本端接口作为 Client 端接受由对端（Server 端）分配的 IP 地址。该方式主要用于设备在通过 ISP 访问 Internet 时，由 ISP 分配 IP 地址。
- Server 端：若设备作为 Server 端为 Client 端分配 IP 地址，则应先配置地址池（可以是 PPP 地址池或者 DHCP 地址池），然后在 ISP 域下关联地址池，或者在接口下指定为 Client 端分配的 IP 地址或者地址池，最后再配置 Server 端的 IP 地址，开始进行 IPCP 协商。

当 Client 端配置了 IP 地址可协商属性后，Server 端根据 AAA 认证结果（关于 AAA 的介绍请参见“安全配置指导”中的“AAA”）和接口下的配置，按照如下顺序给 Client 端分配 IP 地址：

- 如果 AAA 认证服务器为 Client 端设置了 IP 地址或者地址池信息，则 Server 端将采用此信息为 Client 端分配 IP 地址（这种情况下，为 Client 端分配的 IP 地址或者分配 IP 地址所采用的地址池信息是在 AAA 认证服务器上进行配置的，Server 端不需要进行特殊配置）。
- 如果 Client 端认证时使用的 ISP 域下设置了为 Client 端分配 IP 地址的地址池，则 Server 端将采用此地址池为 Client 端分配 IP 地址。
- 如果 Server 端的接口下指定了为 Client 端分配的 IP 地址或者地址池，则 Server 端将采用此信息为 Client 端分配 IP 地址。

(2) DNS 服务器地址协商

设备在进行 IPCP 协商的过程中可以进行 DNS 服务器地址协商。设备既可以作为 Client 端接收其它设备分配的 DNS 服务器地址，也可以作为 Server 端向其它设备提供 DNS 服务器地址。通常情况下：

- 当主机与设备通过 PPP 协议相连时，设备应配置为 Server 端，为对端主机指定 DNS 服务器地址，这样主机就可以通过域名直接访问 Internet；
- 当设备通过 PPP 协议连接运营商的接入服务器时，设备应配置为 Client 端，被动接收或主动请求接入服务器指定 DNS 服务器地址，这样设备就可以使用接入服务器分配的 DNS 来解析域名。

4. PPP支持IPv6

在 IPv6 网络中，PPP 进行 IPv6CP 协商过程中，只协商出 IPv6 接口标识，不能协商出 IPv6 地址、IPv6 DNS 服务器地址。

(1) IPv6 地址分配

PPP 进行 IPv6CP 协商过程中，只协商出 IPv6 接口标识，不能直接协商出 IPv6 地址。

客户端可以通过如下三种方式分配到 IPv6 全球单播地址：

- 方式 1：客户端通过 ND 协议中的 RA 报文获得 IPv6 地址前缀。客户端采用 RA 报文中携带的前缀和 IPv6CP 协商的 IPv6 接口标识一起组合生成 IPv6 全球单播地址。RA 报文中携带的 IPv6 地址前缀的来源有三种：AAA 授权的 IPv6 前缀、接口下配置的 RA 前缀、接口下配置的 IPv6 全球单播地址的前缀。三种来源的优先级依次降低，AAA 授权的优先级最高。关于 ND 协议的详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

- 方式 2：客户端通过 DHCPv6 协议申请 IPv6 全球单播地址。在服务器端可以通过 AAA 授权为每个客户端分配不同的地址池，当授权了地址池后，DHCPv6 在分配 IPv6 地址时会从地址池中获取 IPv6 地址分配给客户端。如果 AAA 未授权地址池，DHCPv6 会根据服务器端的 IPv6 地址查找匹配的地址池为客户端分配地址。
- 方式 3：客户端通过 DHCPv6 协议申请代理前缀，客户端通过代理前缀为下面的主机分配 IPv6 全球单播地址。代理前缀分配方式中地址池的选择原则和通过 DHCPv6 协议分配 IPv6 全球单播地址方式中地址池的选择原则一致。

根据组网不同，主机获取 IPv6 地址的方式如下：

- 当主机通过桥设备或者直连接入设备时，设备可以采用上述的方式 1 或方式 2 直接为主机分配 IPv6 全球单播地址。
- 当主机通过路由器接入设备时，设备可以采用方式 3 为路由器分配 IPv6 前缀，路由器把这些 IPv6 前缀分配给主机来生成 IPv6 全球单播地址。

(2) IPv6 DNS 服务器地址分配

在 IPv6 网络中，IPv6 DNS 服务器地址的分配有如下两种方式：

- AAA 授权 IPv6 DNS 服务器地址，通过 ND 协议中的 RA 报文将此 IPv6 DNS 服务器地址分配给主机。
- DHCPv6 客户端向 DHCPv6 服务器申请 IPv6 DNS 服务器地址。

1.2 配置PPP

1.2.1 PPP配置任务简介

表1-1 PPP 配置任务简介

配置任务	说明	详细配置
配置PPP认证方式	可选	1.2.2
配置轮询功能	可选	1.2.3
配置PPP协商参数	可选	1.2.4
配置PPP IPHC压缩功能	可选	1.2.5
配置PPP计费统计功能	可选	1.2.6
配置PPP用户的nas-port-type属性	可选	1.2.7

1.2.2 配置PPP认证方式

PPP 支持如下认证方式：PAP、CHAP、MSCHAP、MSCHAPv2。用户可以同时配置多种认证方式，在 LCP 协商过程中，认证方根据用户配置的认证方式顺序逐一与被认证方进行协商，直到协商通过。如果协商过程中，被认证方回应的协商报文中携带了建议使用的认证方式，认证方查找配置中存在该认证方式，则直接使用该认证方式进行认证。

1. 配置PAP认证

(1) 配置认证方

表1-2 配置认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为PAP	**ppp authentication-mode pap** [[**call-in**] **domain** *isp-name*]	缺省情况下，PPP协议不进行认证
配置本地AAA认证或者远程AAA认证	请参见“安全配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名和密码必须与被认证方上的配置一致 查看加密方式时，无论采用明文加密方式还是密文加密方式，默认显示为密文加密方式

(2) 配置被认证方

表1-3 配置被认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地被对端以PAP方式认证时本地发送的PAP用户名和密码	**ppp pap local-user** *username* **password** { **cipher** | **simple** } *password*	缺省情况下，被对端以PAP方式认证时，本地设备发送的用户名和密码均为空

2. 配置CHAP认证

CHAP 认证分为两种：认证方配置了用户名和认证方没有配置用户名。

(1) 认证方配置了用户名

- 配置认证方

表1-4 配置认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为CHAP	**ppp authentication-mode chap** [[**call-in**] **domain** *isp-name*]	缺省情况下，PPP协议不进行认证
配置采用CHAP认证时认证方的用户名	**ppp chap user** *username*	缺省情况下，CHAP认证的用户名为空 在被认证方上为认证方配置的用户名必须跟此处配置的一致

操作	命令	说明
配置本地AAA认证或者远程AAA认证	请参见“安全配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名必须与被认证方上的配置一致 认证方用户的密码和被认证方用户的密码要配置成相同的

- 配置被认证方

表1-5 配置被认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置采用CHAP认证时被认证方的用户名	**ppp chap user** *username*	缺省情况下，CHAP认证的用户名为空 在认证方上为被认证方配置的用户名必须跟此处配置的一致
配置本地AAA认证或者远程AAA认证	请参见“安全配置指导”中的“AAA” • 若采用本地 AAA 认证，则被认证方必须为认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置认证方的用户名和密码	为认证方配置的用户名必须与认证方上的配置一致 认证方用户的密码和被认证方用户的密码要配置成相同的

(2) 认证方没有配置用户名

- 配置认证方

表1-6 配置认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为CHAP	**ppp authentication-mode chap** [[**call-in**] **domain** *isp-name*]	缺省情况下，PPP协议不进行认证
配置本地AAA认证或者远程AAA认证	请参见“安全配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名必须与被认证方上的配置一致 为被认证方配置的密码必须与被认证方上配置的CHAP认证密码一致

- 配置被认证方

表1-7 配置被认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置采用CHAP认证时被认证方的用户名	**ppp chap user** *username*	缺省情况下，CHAP认证的用户名为空 在认证方上为被认证方配置的用户名必须跟此处配置的一致
设置CHAP认证密码	**ppp chap password** { **cipher** | **simple** } *password*	缺省情况下，没有配置进行CHAP认证时采用的密码 在认证方上为被认证方配置的密码必须跟此处配置的一致 查看加密方式时，无论采用明文加密方式还是密文加密方式，默认显示为密文加密方式

3. 配置MSCHAP或MSCHAPv2 认证

与 CHAP 认证相同，MSCHAP 和 MSCHAPv2 认证也分为两种：认证方配置了用户名和认证方没有配置用户名。

配置 MSCHAP 或 MSCHAPv2 认证时需注意：

- 设备只能作为 MSCHAP 和 MSCHAPv2 的认证方来对其它设备进行认证。
- L2TP 环境下仅支持 MSCHAP 认证，不支持 MSCHAPv2 认证。
- MSCHAPv2 认证只有在 RADIUS 认证的方式下，才能支持修改密码机制。

表1-8 配置 MSCHAP 或 MSCHAPv2 认证的认证方（认证方配置了用户名）

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为MSCHAP或MSCHAPv2	**ppp authentication-mode** { **ms-chap** | **ms-chap-v2** } [[**call-in**] **domain** *isp-name*]	缺省情况下，PPP协议不进行认证
配置采用MSCHAP或MSCHAPv2认证时认证方的用户名	**ppp chap user** *username*	在被认证方上为认证方配置的用户名必须跟此处配置的一致
配置本地AAA认证或者远程AAA认证	请参见“安全配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名和密码必须与被认证方上的配置一致

表1-9 配置 MSCHAP 或 MSCHAPv2 认证的认证方（认证方没有配置用户名）

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为MSCHAP或MSCHAPv2	**ppp authentication-mode** { **ms-chap** | **ms-chap-v2** } [[**call-in**] **domain** *isp-name*]	缺省情况下，PPP协议不进行认证
配置本地AAA认证或者远程AAA认证	请参见“安全配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名和密码必须与被认证方上的配置一致

1.2.3 配置轮询功能

PPP 协议使用轮询机制来确认链路状态是否正常。

当接口上封装的链路层协议为 PPP 时，链路层会周期性地向对端发送 keepalive 报文（可以通过 **timer-hold** 命令修改 keepalive 报文的发送周期）。如果接口在 *retry* 个（可以通过 **timer-hold retry** 命令修改该个数）keepalive 周期内无法收到对端发来的 keepalive 报文，链路层会认为对端故障，上报链路层 Down。

如果将 keepalive 报文的发送周期配置为 0 秒，则不发送 keepalive 报文。

在速率非常低的链路上，keepalive 周期和 *retry* 值不能配置过小。因为在低速链路上，大报文可能会需要很长的时间才能传送完毕，这样就会延迟 keepalive 报文的发送与接收。而接口如果在 *retry* 个 keepalive 周期之后仍然无法收到对端的 keepalive 报文，它就会认为链路发生故障。如果 keepalive 报文被延迟的时间超过接口的这个限制，链路就会被认为发生故障而被关闭。

表1-10 配置轮询功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口发送keepalive报文的周期	**timer-hold** *seconds*	缺省情况下，接口发送keepalive报文的周期为10秒
配置接口在多少个keepalive周期内没有收到keepalive报文的应答就拆除链路	**timer-hold retry** *retry*	缺省情况下，接口在5个keepalive周期内没有收到keepalive报文的应答就拆除链路

1.2.4 配置PPP协商参数

可以配置的 PPP 协商参数包括：

- 协商超时时间间隔

- 协商 IP 地址
- 协商接口 IP 网段
- 协商 DNS 服务器地址

1. 配置协商超时时间间隔

在 PPP 协商过程中，如果在这个时间间隔内没有收到对端的应答报文，则 PPP 将会重发前一次发送的报文。超时时间间隔的取值范围为 1～10 秒。

在 PPP 链路两端设备对 LCP 协商报文的处理速度差异较大的情况下，为避免因一端无法及时处理对端发送的 LCP 协商报文而导致对端重传，可在对协商报文处理速度较快的设备上配置 LCP 协商的延迟时间。配置 LCP 协商的延时时间后，当接口物理层 UP 时 PPP 将在延时时间超时后才会主动进行 LCP 协商；如果在延时时间内本端设备收到对端设备发送的 LCP 协商报文，则本端设备将不再等待延时时间超时，而是直接进行 LCP 协商。

表1-11 配置协商超时时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置协商超时时间间隔	**ppp timer negotiate** *seconds*	缺省情况下，协商超时时间间隔为3秒
（可选）配置LCP协商的延迟时间	**ppp lcp delay** *milliseconds*	缺省情况下，接口物理层UP后，PPP立即进行LCP协商

2. 配置PPP协商IP地址

(1) 配置 Client 端

表1-12 配置 Client 端

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
为接口配置IP地址可协商属性	**ip address ppp-negotiate**	缺省情况下，接口没有配置IP地址可协商属性 本命令和**ip address**命令互斥，二者不能同时配置。关于**ip address**命令的详细介绍，请参见“三层技术-IP业务命令参考”中的“IP地址”

(2) 配置 Server 端

在下列三种 Server 端分配 IP 地址的方式下 Server 端需要进行配置：

- 在接口下指定为 Client 端分配的 IP 地址。
- 从接口下指定的地址池中分配 IP 地址。
- 从 ISP 域下关联的地址池中分配 IP 地址。

这三种方式中，不同 PPP 用户可以采用的方式如下：

- 不需要进行 PPP 认证的 PPP 用户可以使用两种方式：在接口下指定为 Client 端分配的 IP 地址和从接口下指定的地址池中分配 IP 地址。这两种方式不能同时使用。
- 需要进行 PPP 认证的 PPP 用户可以使用全部的三种方式。用户可以同时配置多种方式。同时配置多种方式时，以 ISP 域下关联的地址池优先，然后是接口下指定为 Client 端分配的 IP 地址或者地址池（接口下的这两种方式不能同时使用）。

PPP 可以使用两类地址池为对端分配 IP 地址：PPP 地址池、DHCP 地址池，优先采用 PPP 地址池。如果用户配置了名称相同的 PPP 地址池和 DHCP 地址池，并采用该名称的地址池来分配 IP 地址，则系统只会使用 PPP 地址池来分配 IP 地址。

表1-13 配置 Server 端（在接口下指定为 Client 端分配的 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口为Client端分配的IP地址	**remote address** *ip-address*	缺省情况下，接口不为Client端分配IP地址
配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址

表1-14 配置 Server 端（从接口下指定的 PPP 地址池中分配 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-
配置PPP地址池	**ip pool** *pool-name start-ip-address* [*end-ip-address*] [**group** *group-name*]	缺省情况下，没有配置PPP地址池
（可选）配置PPP地址池的网关地址	**ip pool** *pool-name* **gateway** *ip-address*	缺省情况下，没有为PPP地址池配置网关地址
（可选）配置PPP地址池路由	**ppp ip-pool route** *ip-address* { *mask-length* | *mask* }	缺省情况下，没有配置PPP地址池路由 用户需要保证配置的PPP地址池路由网段覆盖PPP地址池网段范围
进入接口视图	**interface** *interface-type interface-number*	-
使用PPP地址池为Client端分配IP地址	**remote address pool** *pool-name*	缺省情况下，接口不为Client端分配IP地址
（可选）配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址 配置了PPP地址池的网关地址后，可以不用配置本命令

表1-15 配置 Server 端（从接口下指定的 DHCP 地址池中分配 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
使用DHCP地址池为Client端分配IP地址	**remote address pool** *pool-name*	缺省情况下，接口不为Client端分配IP地址
配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址
（可选）配置使用PPP用户名作为DHCP客户端ID	**remote address dhcp client-identifier username**	缺省情况下，未使用PPP用户名作为DHCP客户端ID

表1-16 配置 Server 端（从 ISP 域下关联的 PPP 地址池中分配 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-
配置PPP地址池	**ip pool** *pool-name start-ip-address* [*end-ip-address*] **group** *group-name*	缺省情况下，没有配置PPP地址池
（可选）配置PPP地址池的网关地址	**ip pool** *pool-name* **gateway** *ip-address*	缺省情况下，没有为PPP地址池配置网关地址
（可选）配置PPP地址池路由	**ppp ip-pool route** *ip-address* { *mask-length* | *mask* }	缺省情况下，没有配置PPP地址池路由 用户需要保证配置的PPP地址池路由网段覆盖PPP地址池网段范围
进入ISP域视图	**domain** *isp-name*	-
在ISP域下关联PPP地址池为Client端分配IP地址	**authorization-attribute ip-pool** *pool-name*	缺省情况下，ISP域下没有关联PPP地址池 本命令的详细介绍请参见“安全命令参考”中的“AAA”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
（可选）配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址 配置了PPP地址池的网关地址后，可以不用配置本命令

表1-17 配置 Server 端（从 ISP 域下关联的 DHCP 地址池中分配 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
在ISP域下关联DHCP地址池为Client端分配IP地址	**authorization-attribute ip-pool** *pool-name*	缺省情况下，ISP域下没有关联DHCP地址池 本命令的详细介绍请参见“安全命令参考”中的“AAA”

操作	命令	说明
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址
（可选）配置使用PPP用户名作为DHCP客户端ID	**remote address dhcp client-identifier username**	缺省情况下，未使用PPP用户名作为DHCP客户端ID

3. 配置接口IP网段检查

使能接口的 IP 网段检查功能后，当 IPCP 协商时，本地会检查对端的 IP 地址与本端接口的 IP 地址是否在同一网段，如果不在同一网段，则 IPCP 协商失败。

如果接口的 IP 网段检查功能处于关闭状态，则在 IPCP 协商阶段不进行接口 IP 网段检查。

表1-18 配置接口 IP 网段检查

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能接口的IP网段检查功能	**ppp ipcp remote-address match**	缺省情况下，接口的IP网段检查功能处于关闭状态

4. 配置DNS服务器地址协商

(1) 配置 Client 端

正常情况下，Client 端配置了 **ppp ipcp dns request** 命令，Server 端才会为本端指定 DNS 服务器地址。但是有一些特殊的设备，Client 端并未请求，Server 端却要强制为 Client 端指定 DNS 服务器地址，从而导致协商不通过，为了适应这种情况，Client 端可以配置 **ppp ipcp dns admit-any** 命令。

表1-19 配置 Client 端

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置设备主动请求对端指定DNS服务器地址	**ppp ipcp dns request**	缺省情况下，禁止设备主动向对端请求DNS服务器地址
配置设备可以被动地接收对端指定的DNS服务器地址，即设备不发送DNS请求，也能接收对端设备分配的DNS服务器地址	**ppp ipcp dns admit-any**	缺省情况下，设备不会被动地接收对端设备指定的DNS服务器的IP地址 在配置了**ppp ipcp dns request**命令的情况下不用配置本命令

(2) 配置 Server 端

表1-20 配置 Server 端

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置设备为对端设备指定DNS服务器地址	**ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]	缺省情况下，设备不为对端设备指定DNS服务器的IP地址 收到Client端的请求后，Server端才会为对端指定DNS服务器地址

1.2.5 配置PPP IPHC压缩功能

IPHC（IP Header Compression，IP 报文头压缩）协议主要应用于低速链路上的语音通信。

在低速链路上，每个语音报文中报文头消耗大部分的带宽。比如，G.729 编码 20ms 打包时长 PPP 链路，每秒传送 1000/20=50 个语音报文，每个语音报文中都包含 46 字节的报文头（6 字节 PPP 头、20 字节 IP 头、8 字节 UDP 头、12 字节 RTP 头），这样每一路语音数据所占的带宽为：（6+20+8+12）*8*50+8000（语音净荷所占带宽）=26.4kbps，传送 RTP/UDP/IP 头所花的带宽开销还是很大的，为（20+8+12）*8*50=16kbps，占语音数据总带宽的百分比为 16k/26.4k=60.1%，网络带宽利用率很差。为了减少报文头对带宽的消耗，可以在 PPP 链路上使用 IPHC 压缩功能，对报文头进行压缩。

IPHC 压缩分为如下两种：

- RTP 头压缩：对报文中的 RTP/UDP/IP 头（长度共 40 字节）进行压缩。
- TCP 头压缩：对报文中的 TCP/IP 头（长度共 40 字节）进行压缩。

IPHC 压缩机制的总体思想是：在一次连接过程中，IP 头、UDP 头、RTP 头以及 TCP 头中的一些字段是固定不变的，还有一些字段是有规律变化的，这样在压缩端和解压端分别维护一个压缩表项和解压缩表项来保存固定不变的字段和有规律变化的字段，在传输过程中，压缩端不需要发送完整的报文头，只发送报文头中有变化的信息，减少了报文头信息的长度，从而降低了报文头所占的带宽。

(1) 在压缩过程中，压缩端会将变化的字段编码到报文中；对于有规律变化的字段，其二次差分值为零时则不需要携带，其二次差分值不为零时，则其标志位置 1，并将其一次差分值和标志位字段编码到报文中。

(2) 在解压过程中，解压端跟据解压缩表项还原固定不变的字段，对于有规律变化的字段，若其标志位为 0，则按其变化规律做相应计算还原；若其标志位为 1，则根据报文中携带的该字段的一次差分值和解压缩表项中该字段的信息进行计算还原。

举例说明：在压缩 TCP 头时，Destination Port 为固定不变的字段，在报文中不用携带；URG 为变化的字段，在报文中携带；Sequence Number 为有规律变化的字段（一般情况下是每次增加 1），压缩端首先计算被压缩报文的 Sequence Number 字段和压缩表项中的 Sequence Number 字段的差值，即一次差分值，如果一次差分值为 1，那么其二次差分值为 1-1=0，则这个字段就不用携带，解压端会自动加 1 还原；如果其一次差分值不为 1，比如为 2，那么二次差分值就为 2-1=1，这时

就会置位 Sequence Number 的标志位，并将一次差分值 2 编码到报文中，解压端会在解压缩表项中的 Sequence Number 字段上加 2 还原。

配置本功能时需要注意：

- 用户必须在链路的两端同时开启 IPHC 压缩功能，该功能才生效。
- 在虚拟模板接口、Dialer 接口上开启/关闭 IPHC 压缩功能时，配置不会立即生效，只有对此接口或者其绑定的物理接口进行 **shutdown/undo shutdown** 操作后，配置才能生效。
- 只有在开启 IPHC 压缩功能后，才能配置接口上允许进行 RTP 头/TCP 头压缩的最大连接数，并且需要对接口进行 **shutdown/undo shutdown** 操作后，配置才能生效。在关闭 IPHC 压缩功能后，配置将被清除。

表1-21 配置 PPP IPHC 压缩功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启PPP IPHC压缩功能	**ppp compression iphc enable** [**nonstandard**]	缺省情况下，IPHC压缩功能处于关闭状态 与友商设备互通时需要配置**nonstandard**参数
配置接口上允许进行RTP头压缩的最大连接数	**ppp compression iphc rtp-connections** *number*	缺省情况下，接口上允许进行RTP头压缩的最大连接数为16
配置接口上允许进行TCP头压缩的最大连接数	**ppp compression iphc tcp-connections** *number*	缺省情况下，接口上允许进行TCP头压缩的最大连接数为16

1.2.6 配置PPP计费统计功能

PPP 协议可以为每条 PPP 链路提供基于流量的计费统计功能，具体统计内容包括出入两个方向上流经本链路的报文数和字节数。AAA 可以获取这些流量统计信息用于计费控制。关于 AAA 计费的详细介绍请参见“安全配置指导”中的“AAA”。

表1-22 配置 PPP 计费统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启PPP计费统计功能	**ppp account-statistics enable** [**acl** { *acl-number* | **name** *acl-name* }]	缺省情况下，PPP计费统计功能处于关闭状态

1.2.7 配置PPP用户的nas-port-type属性

本特性用来配置 RADIUS 认证计费时所携带的 nas-port-type 属性。关于 nas-port-type 属性的详细介绍请参见 RFC 2865。

表1-23 配置 PPP 用户的 nas-port-type 属性

操作	命令	说明
进入系统视图	**system-view**	-
进入虚拟模板接口视图	**interface virtual-template** *number*	-
配置接口的nas-port-type属性	**nas-port-type** { **802.11** | **adsl-cap** | **adsl-dmt** | **async** | **cable** | **ethernet** | **g.3-fax** | **hdlc** | **idsl** | **isdn-async-v110** | **isdn-async-v120** | **isdn-sync** | **piafs** | **sdsl** | **sync** | **virtual** | **wireless-other** | **x.25** | **x.75** | **xdsl** }	缺省情况下，nas-port-type属性由PPP用户的业务类型和承载链路类型决定： • 如果是 PPPoE 业务，当承载链路类型为三层虚拟以太网接口时，nas-port-type 属性为 **xdsl**，否则 nas-port-type 属性为 **ethernet** • 如果是 PPPoA 业务，nas-port-type 属性为 **xdsl** • 如果是 L2TP 业务，nas-port-type 属性为 **virtual**

1.3 PPP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 PPP 和 MP 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除相应接口的统计信息。

表1-24 PPP 和 MP 显示和维护

操作	命令
显示PPP接入用户的信息	**display ppp access-user** { **interface** *interface-type interface-number* [**count**] | **ip-address** *ip-address* | **ipv6-address** *ipv6-address* | **username** *user-name* | **user-type** { **lac** | **lns** | **pppoa** | **pppoe** } [**count**] }
显示PPP地址池的信息	**display ip pool** [*pool-name* | **group** *group-name*]
显示IPHC压缩的统计信息	**display ppp compression iphc** { **rtp** | **tcp** } [**interface** *interface-type interface-number*]
显示虚拟模板接口的相关信息	**display interface** [**virtual-template** [*interface-number*]] [**brief** [**description** | **down**]]
显示虚拟访问接口的相关信息	**display interface** [**virtual-access** [*interface-number*]] [**brief** [**description** | **down**]]
清除IPHC压缩的统计信息	**reset ppp compression iphc** [**rtp** | **tcp**] [**interface** *interface-type interface-number*]
强制PPP用户下线	**reset ppp access-user** { **ip-address** *ip-address* | **ipv6-address** *ipv6-address* | **username** *user-name* }
清除VA接口的统计信息	**reset counters interface** [**virtual-access** [*interface-number*]]

2 PPPoE


说明

WX1800H 系列、WX2500H 系列和 WX3000H 系列不支持 slot 参数。

2.1 PPPoE简介

PPPoE（Point-to-Point Protocol over Ethernet，在以太网上承载 PPP 协议）的提出，解决了 PPP 无法应用于以太网的问题，是对 PPP 协议的扩展。

2.1.1 PPPoE概述

PPPoE 描述了在以太网上建立 PPPoE 会话及封装 PPP 报文的方法。要求通信双方建立的是点到点关系，而不是在以太网中所出现的点到多点关系。

PPPoE 利用以太网将大量主机组成网络，然后通过一个远端接入设备为以太网上的主机提供互联网接入服务，并对接入的每台主机实现控制、认证、计费功能。由于很好地结合了以太网的经济性及 PPP 良好的可扩展性与管理控制功能，PPPoE 被广泛应用于小区接入组网等环境中。

PPPoE 协议将 PPP 报文封装在以太网帧之内，在以太网上提供点对点的连接。

关于 PPPoE 的详细介绍，可以参考 RFC 2516。

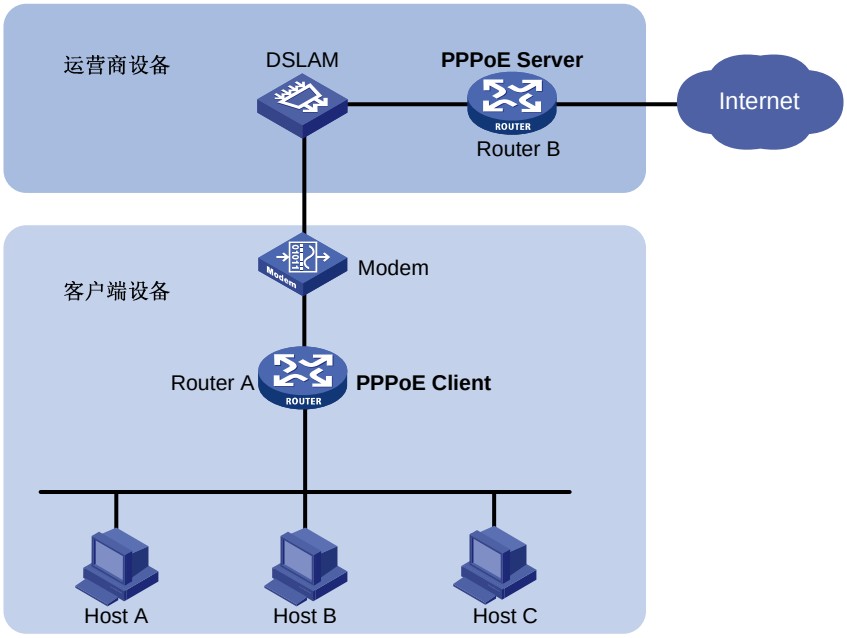
2.1.2 PPPoE组网结构

PPPoE 使用 Client/Server 模型。PPPoE Client 向 PPPoE Server 发起连接请求，两者之间会话协商通过后，就建立 PPPoE 会话，此后 PPPoE Server 向 PPPoE Client 提供接入控制、认证、计费等功能。

根据 PPPoE 会话的起点所在位置的不同，有两种组网结构：

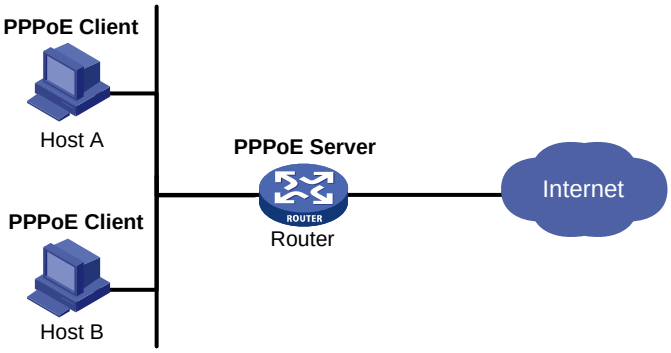
- 第一种方式是在两台路由器之间建立 PPPoE 会话，所有主机通过同一个 PPPoE 会话传送数据，主机上不用安装 PPPoE 客户端拨号软件，一般是一个企业共用一个账号接入网络（图中 PPPoE Client 位于企业/公司内部，PPPoE Server 是运营商的设备）。

图2-1 PPPoE 组网结构图 1



- 第二种方式是将 PPPoE 会话建立在 Host 和运营商的路由器之间，为每一个 Host 建立一个 PPPoE 会话，每个 Host 都是 PPPoE Client，每个 Host 使用一个帐号，方便运营商对用户进行计费和控制。Host 上必须安装 PPPoE 客户端拨号软件。

图2-2 PPPoE 组网结构图 2



2.2 配置PPPoE

设备作为PPPoE Server时，配置过程请参见“2.2.1 配置PPPoE Server”。

设备作为PPPoE Client时，配置过程请参见“2.2.2 配置PPPoE Client”。

2.2.1 配置PPPoE Server

1. 配置PPPoE会话

表2-1 配置 PPPoE 会话

操作	命令	说明
进入系统视图	**system-view**	-
创建虚拟模板接口并进入指定的虚拟模板接口视图	**interface virtual-template** *number*	如果指定的虚拟模板接口已经创建，则该命令用来直接进入虚拟模板接口视图
设置PPP的工作参数（包括：认证方式、IP地址获取方式，用户还可以设置为PPP对端分配的IP地址或使用地址池为PPP对端分配IP地址）	请参见“1.2 配置PPP”	如果配置认证，PPPoE Server需作为认证方
开启PPPoE应用的MRU检测功能	**ppp lcp echo mru verify** [**minimum** *value*]	PPPoE应用的MRU检测功能处于关闭状态
退回系统视图	**quit**	-
VLAN接口视图	**interface** *interface-type interface-number*	-
在接口上启用PPPoE Server协议，将该接口与指定的虚拟模板接口绑定	**pppoe-server bind virtual-template** *number*	缺省情况下，接口上的PPPoE Server协议处于关闭状态
（可选）配置PPPoE Server的AC Name（Access Concentrator Name，接入集中器名称）	**pppoe-server tag ac-name** *name*	缺省情况下，PPPoE Server的AC Name为设备名称 PPPoE Client可以根据AC Name来选择PPPoE Server（H3C实现的PPPoE Client暂不支持该功能）
（可选）使能对PPP最大负载TAG的支持，并指定最大负载的范围	**pppoe-server tag ppp-max-payload** [**minimum** *minvalue* **maximum** *maxvalue*]	缺省情况下，不支持PPP最大负载TAG
（可选）配置PPPoE Server的Service Name	**pppoe-server tag service-name** *name*	缺省情况下，PPPoE Server的Service Name为空
（可选）配置用户接入响应延迟时间	**pppoe-server access-delay** *delay-time*	缺省情况下，对用户接入响应不延时
退回系统视图	**quit**	-
配置PPPoE Server对PPP用户进行认证、授权、计费	相关内容请参见“安全配置指导”中的“AAA”	-

2. 限制创建PPPoE会话的数目

系统创建 PPPoE 会话时，需同时满足如下限制，若其中任何一项不满足，则无法创建会话：

- 接口下每个用户所能创建 PPPoE 会话的最大数目限制
- 接口下每个 VLAN 所能创建 PPPoE 会话的最大数目限制
- 接口上所能创建 PPPoE 会话的最大数目限制

- 成员设备所能创建 PPPoE 会话的最大数目限制

本功能配置后仅对新创建的 PPPoE 会话有效，对已经创建的 PPPoE 会话无效，即不会导致已经上线的用户下线。

建议设备上配置的所有成员设备所能创建 PPPoE 会话的最大数目之和，不要超过整机 PPPoE 的最大会话数（整机 PPPoE 的最大会话数由设备的缺省规格或授权的 License 规格决定），否则会有部分 PPPoE 用户因为整机最大用户数已达到而无法上线。

表2-2 限制创建 PPPoE 会话的数目

操作	命令	说明
进入系统视图	**system-view**	-
VLAN接口视图	**interface** *interface-type interface-number*	该接口为启用PPPoE Server协议的接口 -
配置接口上所能创建PPPoE会话的最大数目	**pppoe-server session-limit** *number*	缺省情况下，不限制接口上所能创建PPPoE会话的数目
配置在接口下，每个VLAN所能创建PPPoE会话的最大数目	**pppoe-server session-limit per-vlan** *number*	缺省情况下，不限制每个VLAN所能创建PPPoE会话的数目
配置在接口下，每个用户所能创建PPPoE会话的最大数目	**pppoe-server session-limit per-mac** *number*	缺省情况下，每个用户可创建100个PPPoE会话
退回系统视图	**quit**	-
配置成员设备所能创建PPPoE会话的最大数目	**pppoe-server session-limit slot** *slot-number* **total** *number*	缺省情况下，不限制成员设备所能创建PPPoE会话的数目

3. 限制用户创建PPPoE会话的速度

设备可以限制特定接口下每个用户（每个用户通过 MAC 地址进行标识）创建会话的速度。如果用户建立会话的速度达到门限值，即在监视时间段内该用户的会话请求数目超过配置的允许数目，则扼制该用户的会话请求，即在监视时间段内该用户的超出允许数目的请求都会被丢弃，并输出对应的 Log 信息。如果扼制时间配置为 0，表示不扼制会话请求，但仍然会输出 Log 信息。

系统使用监控表和扼制表来共同控制用户创建会话的速度：

- 监视表：监视各用户在监视时间周期内创建的会话数。监视表的规格为 8K。当监视表达到规格时，对新用户的会话请求不进行监视和扼制，正常建立会话。监视表项的老化时间为配置的 *session-request-period* 值，老化后对用户重新监视。
- 扼制表：当某用户建立会话的速度超过门限值时，会将该用户的信息加入扼制表，扼制该用户的会话请求。扼制表规格为 8K。当扼制表达到规格时，对新用户的会话请求只进行监视和发送 Log 信息，但不触发扼制。扼制表项的老化时间为配置的 *blocking-period* 值，老化后对用户重新监视。

修改本功能的配置后，系统将删除已记录的监视表和扼制表，重新开始监视每个用户的会话请求。

表2-3 限制用户创建 PPPoE 会话的速度

操作	命令	说明
进入系统视图	**system-view**	-
VLAN接口视图	**interface** *interface-type interface-number*	该接口为启用PPPoE Server协议的接口
配置接口允许每个用户创建会话的速度	**pppoe-server throttle per-mac** *session-requests session-request-period blocking-period*	缺省情况下，不限制会话建立的速度
显示被扼制的用户信息	**display pppoe-server throttled-mac** { **slot** *slot-number* | **interface** *interface-type interface-number* }	**display**命令可以在任意视图执行

4. 配置PPPoE会话的nas-port-id属性相关参数

在含有 DSLAM 的组网中，DSLAM 通过接入线路 ID（access-line-id）把用户的物理位置信息传送给 BAS 设备（PPPoE Server 功能部署在 BAS 设备上），接入线路 ID 的内容包括 circuit-id 和 remote-id 两部分。BAS 设备采用一定的规则解析接入线路 ID 后，把解析后的内容通过 RADIUS 的 nas-port-id 属性发送给 RADIUS 服务器，RADIUS 服务器通过收到的 nas-port-id 属性和数据库中已配置好的物理位置信息比较，验证用户的物理位置信息是否正确。

用户可以通过下面的配置控制 BAS 设备上传给 RADIUS 服务器的 nas-port-id 属性的内容。

表2-4 配置 PPPoE 会话的 nas-port-id 属性相关参数

操作	命令	说明
进入系统视图	**system-view**	-
VLAN接口视图	**interface** *interface-type interface-number*	该接口为启用PPPoE Server协议的接口
配置上传给RADIUS服务器的nas-port-id属性中包含的内容	**pppoe-server access-line-id content** { **all** [*separator*] | **circuit-id** | **remote-id** }	缺省情况下，上传给RADIUS服务器的nas-port-id属性中仅包含circuit-id
配置在nas-port-id属性中自动插入BAS信息	**pppoe-server access-line-id bas-info** [**cn-163**]	缺省情况下，在nas-port-id属性中不自动插入BAS信息
配置设备信任接收到的报文中的接入线路ID的内容	**pppoe-server access-line-id trust**	缺省情况下，设备不信任接收到的报文中的接入线路ID的内容
配置接入线路ID中circuit-id的解析格式	**pppoe-server access-line-id circuirt-id parse-mode** { **cn-telecom** | **tr-101** }	缺省情况下，接入线路ID中circuit-id的解析格式为TR-101格式
配置接入线路ID中circuit-id的传输格式	**pppoe-server access-line-id circuit-id trans-format** { **ascii** | **hex** }	缺省情况下，接入线路ID中circuit-id的传输格式为字符串格式
配置接入线路ID中remote-id的传输格式	**pppoe-server access-line-id remote-id trans-format** { **ascii** | **hex** }	缺省情况下，接入线路ID中remote-id的传输格式为字符串格式

5. 配置VA池

PPPoE 在建立连接时需要创建 VA 接口（VA 接口用于 PPPoE 与 PPP 之间的报文传递），在用户下线后需要删除 VA 接口。由于创建/删除 VA 接口需要一定的时间，所以如果有大量用户上线/下线时，PPPoE 的连接建立、连接拆除性能会受到影响。

使用 VA 池对 PPPoE 的连接建立、连接拆除性能有显著提高。VA 池是在建立连接前事先创建的 VA 接口的集合。创建 VA 池后，当需要创建 VA 接口时，直接从 VA 池中获取一个 VA 接口，加快了 PPPoE 连接的建立速度。当用户下线后，直接把 VA 接口放入 VA 池中，不需要删除 VA 接口，加快了 PPPoE 连接的拆除速度。当 VA 池中的 VA 接口耗光后，仍需在建立 PPPoE 连接时再创建 VA 接口，在用户下线后删除 VA 接口。

配置 VA 池时需要注意：

- 每个虚拟模板接口只能关联一个全局 VA 池，在每个成员设备上只能关联一个局部 VA 池。通过某单板上的以太网接口上线的用户，只能使用上线以太网接口绑定的虚拟模板接口在该单板上关联的 VA 池。如果想要修改使用的 VA 池的大小，只能先删除原来的配置，然后重新配置 VA 池。
- 创建/删除 VA 池需要花费一定的时间，请用户耐心等待。在 VA 池创建/删除过程中（还没创建/删除完成）允许用户上线/下线，但正在创建/删除的 VA 池不生效。
- 系统可能由于资源不足不能创建用户指定容量的 VA 池，用户可以通过 **display pppoe-server va-pool** 命令查看实际可用的 VA 池的容量以及 VA 池的状态。
- 删除 VA 池时，如果已有在线用户使用该 VA 池中的 VA 接口，不会导致这些用户下线。

表2-5 配置 VA 池

操作	命令	说明
进入系统视图	**system-view**	-
配置VA池	**pppoe-server virtual-template** *template-number* [**slot** *slot-number*] **va-pool** *va-volume*	缺省情况下，不存在VA池

6. 清除PPPoE会话

在用户视图下执行 **reset pppoe-server** 命令，可在 PPPoE Server 端清除 PPPoE 会话。

表2-6 清除 PPPoE 会话

操作	命令	说明
清除PPPoE会话	**reset pppoe-server** { **all** | **interface** *interface-type interface-number* | **virtual-template** *number* }	-

2.2.2 配置PPPoE Client

PPPoE Client 的配置包括配置拨号接口和配置 PPPoE 会话。

PPPoE 会话有三种工作模式：永久在线模式、按需拨号模式、诊断模式。

- 永久在线模式：当物理线路 up 后，设备会立即发起 PPPoE 呼叫，建立 PPPoE 会话。除非用户删除 PPPoE 会话，否则此 PPPoE 会话将一直存在。

- 按需拨号模式：当物理线路 up 后，设备不会立即发起 PPPoE 呼叫，只有当有数据需要传送时，设备才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果 PPPoE 链路的空闲时间超过用户配置的值，设备会自动中止 PPPoE 会话。
- 诊断模式：设备在配置完成后立即发起 PPPoE 呼叫，建立 PPPoE 会话。每隔用户配置的重建时间间隔，设备会自动断开该会话、并重新发起呼叫建立会话。通过定期建立、删除 PPPoE 会话，可以监控 PPPoE 链路是否处于正常工作状态。

PPPoE 会话的工作模式由对应的拨号接口的配置决定：

- 当 Dialer 接口的链路空闲时间（通过 **dialer timer idle** 命令配置）配置为 0，且 Dialer 接口上没有配置 **dialer diagnose** 命令时，PPPoE 会话将工作在永久在线模式。
- 当 Dialer 接口的链路空闲时间（通过 **dialer timer idle** 命令配置）配置不为 0，且 Dialer 接口上没有配置 **dialer diagnose** 命令时，PPPoE 会话将工作在按需拨号模式。
- 当 Dialer 接口上配置了 **dialer diagnose** 命令时，PPPoE 会话将工作在诊断模式。

1. 配置拨号接口

在配置 PPPoE 会话之前，需要先配置一个 Dialer 接口，并在接口上使能共享 DDR。每个 PPPoE 会话唯一对应一个 Dialer bundle，而每个 Dialer bundle 又唯一对应一个 Dialer 接口。这样就相当于通过一个 Dialer 接口可以创建一个 PPPoE 会话。

表2-7 配置拨号接口

操作	命令	说明
进入系统视图	**system-view**	-
创建拨号访问组，并配置拨号控制规则	**dialer-group** *group-number* **rule** { *protocol-name* { **deny** | **permit** } | **acl** { *acl-number* | **name** *acl-name* } }	缺省情况下，不存在拨号访问组
创建Dialer接口，并进入该Dialer接口视图	**interface dialer** *number*	-
配置接口IP地址	**ip address** { *address mask* | **ppp-negotiate** }	缺省情况下，接口没有配置IP地址
使能共享DDR	**dialer bundle enable**	缺省情况下，接口上不使能任何类型的DDR
配置该拨号接口关联的拨号访问组，将该接口与拨号控制规则关联起来	**dialer-group** *group-number*	缺省情况下，接口不与任何拨号访问组相关联
配置链路空闲时间	**dialer timer idle** *idle* [**in** | **in-out**]	缺省情况下，链路空闲时间为120秒 当*idle*配置为0时，PPPoE会话工作在永久在线模式下，否则工作在按需拨号模式下
配置DDR应用工作在诊断模式	**dialer diagnose** [**interval** *interval*]	缺省情况下，工作在非诊断模式 当工作在诊断模式时，链路空闲时间无效

操作	命令	说明
配置DDR自动拨号的间隔时间	**dialer timer autodial** *autodial-interval*	缺省情况下，DDR自动拨号的间隔时间为300秒 当工作在永久在线模式或者诊断模式情况下，链路断开后将启动自动拨号定时器，等待自动拨号定时器超时后再重新发起呼叫 为了在链路断开时可以尽快自动重新拨号，建议将自动拨号的时间间隔配置的小一些
配置Dialer接口的MTU值	**mtu** *size*	缺省情况下，Dialer接口的MTU值为1500字节 对于PPPoE Client应用的Dialer接口，应修改其MTU值，保证分片后的报文加上2个字节的PPP头和6个字节的PPPoE头之后的总长度不超过对应PPPoE会话所在接口的MTU值

2. 配置PPPoE会话

表2-8 配置 PPPoE 会话

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网接口视图/三层以太网子接口视图/VLAN接口视图/	**interface** *interface-type interface-number*	-
建立一个PPPoE会话，并且指定该会话所对应的Dialer bundle	**pppoe-client dial-bundle-number** *number* [**no-hostuniq**]	缺省情况下，没有配置PPPoE会话 该 Dialer bundle 的序号 *number* 与Dialer接口的编号相同

3. 复位PPPoE会话

当 PPPoE 会话工作在永久在线模式时，如果使用 **reset pppoe-client** 命令复位 PPPoE 会话，设备会在自动拨号定时器超时后自动重新建立 PPPoE 会话。

当 PPPoE 会话工作在按需拨号模式时，如果使用 **reset pppoe-client** 命令复位 PPPoE 会话，设备会在有数据需要传送时，才重新建立 PPPoE 会话。

表2-9 复位 PPPoE 会话

操作	命令	说明
复位PPPoE会话	**reset pppoe-client** { **all** | **dial-bundle-number** *number* }	请在用户视图下进行该操作

2.3 PPPoE显示和维护

2.3.1 PPPoE Server显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 PPPoE Server 配置后的运行情况，通过查看显示信息验证配置的效果。

表2-10 PPPoE Server 显示和维护

操作	命令
显示PPPoE会话的摘要信息	**display pppoe-server session summary** { **slot** *slot-number* | **interface** *interface-type interface-number* }
显示PPPoE会话的数据报文统计信息	**display pppoe-server session packet** { **slot** *slot-number* | **interface** *interface-type interface-number* }
显示被扼制的用户信息	**display pppoe-server throttled-mac** { **slot** *slot-number* | **interface** *interface-type interface-number* }
显示VA池信息	**display pppoe-server va-pool**

2.3.2 PPPoE Client显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 PPPoE Client 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 PPPoE 会话的协议报文统计信息。

表2-11 PPPoE Client 显示和维护

操作	命令
显示PPPoE会话的概要信息	**display pppoe-client session summary** [**dial-bundle-number** *number*]
显示PPPoE会话的协议报文统计信息	**display pppoe-client session packet** [**dial-bundle-number** *number*]
清除PPPoE会话的协议报文统计信息	**reset pppoe-client session packet** [**dial-bundle-number** *number*]

2.4 PPPoE典型配置举例

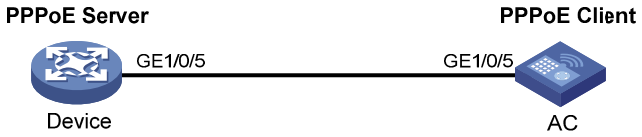
2.4.1 PPPoE Client永久在线模式配置举例

1. 组网需求

Device 和 AC 之间通过各自的 GigabitEthernet1/0/5 接口相连，其中 Device 作为 PPPoE Server，AC 作为 PPPoE Client 工作在永久在线模式。

2. 组网图

图2-3 PPPoE Client 组网图



3. 配置步骤

(1) 配置 Device 作为 PPPoE Server

配置虚拟模板接口 1 的 IP 地址，并指定为对端分配的 IP 地址。

```
<Device> system-view
[Device] interface virtual-template 1
[Device-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[Device-Virtual-Template1] remote address 1.1.1.2
[Device-Virtual-Template1] quit
```

在接口 GigabitEthernet1/0/1 上启用 PPPoE Server 协议，并将该接口与虚拟模板接口 1 绑定。

```
[Device] interface gigabitethernet 1/0/5
[Device-GigabitEthernet1/0/5] pppoe-server bind virtual-template 1
[Device-GigabitEthernet1/0/5] quit
```

(2) 配置 AC 作为 PPPoE Client

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<AC> system-view
[AC] dialer-group 1 rule ip permit
```

在 Dialer1 接口上使能共享 DDR。

```
[AC] interface dialer 1
[AC-Dialer1] dialer bundle enable
```

将 Dialer1 接口与拨号访问组 1 关联。

```
[AC-Dialer1] dialer-group 1
```

配置 Dialer1 接口通过协商获取 IP 地址。

```
[AC-Dialer1] ip address ppp-negotiate
[AC-Dialer1] quit
```

配置一个 PPPoE 会话，该会话对应 Dialer bundle 1（Dialer bundle 1 对应 Dialer1 接口）。

```
[AC] interface gigabitethernet 1/0/5
[AC-GigabitEthernet1/0/5] pppoe-client dial-bundle-number 1
[AC-GigabitEthernet1/0/5] quit
```

配置 PPPoE Client 工作在永久在线模式。

```
[AC] interface dialer 1
[AC-Dialer1] dialer timer idle 0
```

配置 DDR 自动拨号的间隔时间为 60 秒。

```
[AC-Dialer1] dialer timer autodial 60
[AC-Dialer1] quit
```

配置静态路由。

```
[AC] ip route-static 1.1.1.1 255.0.0.0 dialer 1
```

4. 验证配置

配置完成后，AC 就可以与远端的 PPPoE Server 建立 PPPoE 会话。

```
[AC-Dialer1] display pppoe-client session summary
Bundle ID    Interface    VA          RemoteMAC      LocalMAC       State
1      1     GE1/0/5      VA0         00e0-1400-4300 00e0-1500-4100 SESSION
```

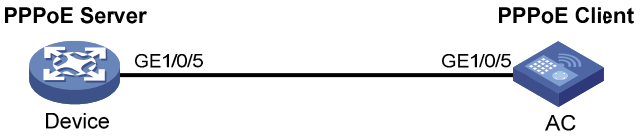
2.4.2 PPPoE Client按需拨号模式配置举例

1. 组网需求

Device 和 AC 之间通过各自的 GigabitEthernet1/0/5 接口相连，其中 Device 作为 PPPoE Server，AC 作为 PPPoE Client 工作在按需拨号模式，空闲时间间隔为 150 秒。

2. 组网图

图2-4 PPPoE Client 组网图



3. 配置步骤

(1) 配置 Device 作为 PPPoE Server

配置虚拟模板接口 1 的 IP 地址，并指定为对端分配的 IP 地址。

```
<Device> system-view
[Device] interface virtual-template 1
[Device-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[Device-Virtual-Template1] remote address 1.1.1.2
[Device-Virtual-Template1] quit
```

在接口 GigabitEthernet1/0/5 上启用 PPPoE Server 协议，并将该接口与虚拟模板接口 1 绑定。

```
[Device] interface gigabitethernet 1/0/5
[Device-GigabitEthernet1/0/5] pppoe-server bind virtual-template 1
[Device-GigabitEthernet1/0/5] quit
```

(2) 配置 AC 作为 PPPoE Client

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<AC> system-view
[AC] dialer-group 1 rule ip permit
```

在 Dialer1 接口上使能共享 DDR。

```
[AC] interface dialer 1
[AC-Dialer1] dialer bundle enable
```

将 Dialer1 接口与拨号访问组 1 关联。

```
[AC-Dialer1] dialer-group 1
```

配置 Dialer1 接口通过协商获取 IP 地址。

```
[AC-Dialer1] ip address ppp-negotiate
[AC-Dialer1] quit
```

配置一个 PPPoE 会话，该会话对应 Dialer bundle 1（Dialer bundle 1 对应 Dialer1 接口）。

```
[AC] interface gigabitethernet 1/0/5
[AC-GigabitEthernet1/0/5] pppoe-client dial-bundle-number 1
[AC-GigabitEthernet1/0/5] quit
```

配置静态路由。

```
[AC] ip route-static 1.1.1.1 255.0.0.0 dialer 1
```

配置空闲时间间隔为 150 秒。

```
[AC] interface dialer 1
[AC-Dialer1] dialer timer idle 150
[AC-Dialer1] quit
```

4. 验证配置

配置完成后，AC 就可以与远端的 PPPoE Server 建立 PPPoE 会话。

```
[AC-Dialer1] display pppoe-client session summary
Bundle ID    Interface    VA          RemoteMAC      LocalMAC       State
1      1     GE1/0/5      VA0         00e0-1400-4300 00e0-1500-4100 SESSION
```

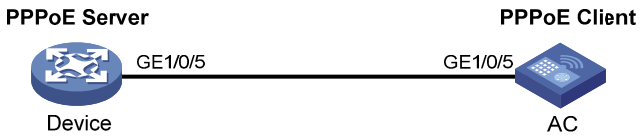
2.4.3 PPPoE Client诊断模式配置举例

1. 组网需求

Device 和 AC 之间通过各自的 GigabitEthernet1/0/5 接口相连，其中 Device 作为 PPPoE Server，AC 作为 PPPoE Client 工作在诊断模式，诊断时间间隔为 200 秒。

2. 组网图

图2-5 PPPoE Client 组网图



3. 配置步骤

(1) 配置 Device 作为 PPPoE Server

配置虚拟模板接口 1 的 IP 地址，并指定为对端分配的 IP 地址。

```
<Device> system-view
[Device] interface virtual-template 1
[Device-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[Device-Virtual-Template1] remote address 1.1.1.2
[Device-Virtual-Template1] quit
```

在接口 GigabitEthernet1/0/5 上启用 PPPoE Server 协议，并将该接口与虚拟模板接口 1 绑定。

```
[Device] interface gigabitethernet 1/0/5
[Device-GigabitEthernet1/0/5] pppoe-server bind virtual-template 1
[Device-GigabitEthernet1/0/5] quit
```

(2) 配置 AC 作为 PPPoE Client

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<AC> system-view
[AC] dialer-group 1 rule ip permit
```
在 Dialer1 接口上使能共享 DDR。
```
[AC] interface dialer 1
[AC-Dialer1] dialer bundle enable
```
将 Dialer1 接口与拨号访问组 1 关联。
```
[AC-Dialer1] dialer-group 1
```
配置 Dialer1 接口通过协商获取 IP 地址。
```
[AC-Dialer1] ip address ppp-negotiate
[AC-Dialer1] quit
```
配置一个 PPPoE 会话，该会话对应 Dialer bundle 1（Dialer bundle 1 对应 Dialer1 接口）。
```
[AC] interface gigabitethernet 1/0/5
[AC-GigabitEthernet1/0/5] pppoe-client dial-bundle-number 1
[AC-GigabitEthernet1/0/5] quit
```
PPPoE Client 工作在诊断模式，诊断时间间隔为 200 秒。
```
[AC] interface dialer 1
[AC-Dialer1] dialer diagnose interval 200
```
配置自动拨号的时间间隔为 10 秒。
```
[AC-Dialer1] dialer timer autodial 10
```

4. 验证配置

配置完成后，AC 就可以与远端的 PPPoE Server 建立 PPPoE 会话。

```
[AC-Dialer1] display pppoe-client session summary
Bundle ID    Interface    VA          RemoteMAC      LocalMAC       State
1      1     GE1/0/5      VA0         00e0-1400-4300 00e0-1500-4100 SESSION
```

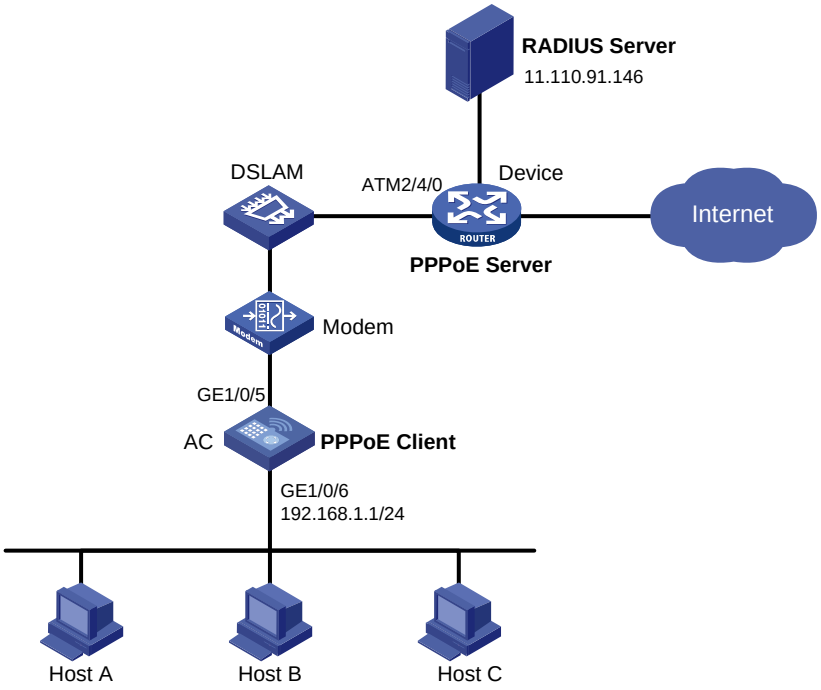
2.4.4 利用ADSL Modem将局域网接入Internet

1. 组网需求

- 局域网内的计算机通过 AC 访问 Internet，AC 通过 ADSL Modem 采用永久在线的方式接入 DSLAM。
- ADSL 帐户的用户名为 user1，密码为 123456。
- Device 作为 PPPoE Server 通过 ATM2/4/0 接口连接至 DSLAM，提供 RADIUS 认证、授权、计费功能。
- 在 AC 上使能 PPPoE Client 功能，局域网内的主机不用安装 PPPoE 客户端软件即可访问 Internet。

2. 组网图

图2-6 利用 ADSL 将局域网接入 Internet 组网图



3. 配置步骤

(1) 配置 AC 作为 PPPoE Client

配置拨号访问组 1 以及对应的拨号访问控制条件。

```
<AC> system-view
[AC] dialer-group 1 rule ip permit
```

在 Dialer1 接口上使能共享 DDR。

```
[AC] interface dialer 1
[AC-Dialer1] dialer bundle enable
```

将 Dialer1 接口与拨号访问组 1 关联。

```
[AC-Dialer1] dialer-group 1
```

配置 Dialer1 接口通过协商获取 IP 地址。

```
[AC-Dialer1] ip address ppp-negotiate
```

配置 PPPoE Client 工作在永久在线模式。

```
[AC-Dialer1] dialer timer idle 0
```

配置本地被 Device 以 PAP 方式认证时 AC 发送的 PAP 用户名和密码。

```
[AC-Dialer1] ppp pap local-user user1 password simple 123456
[AC-Dialer1] quit
```

配置 PPPoE 会话。

```
[AC] interface gigabitethernet 1/0/5
[AC-GigabitEthernet1/0/5] pppoe-client dial-bundle-number 1
[AC-GigabitEthernet1/0/5] quit
```

配置局域网接口的 IP 地址。

```
[AC] interface gigabitethernet 1/0/6
[AC-GigabitEthernet1/0/6] ip address 192.168.1.1 255.255.255.0
[AC-GigabitEthernet1/0/6] quit
```

配置缺省路由。

```
[AC] ip route-static 0.0.0.0 0 dialer 1
```

如果局域网内计算机使用的 IP 地址为私有地址，还需要在设备上配置 NAT（Network Address Translation，网络地址转换）。

(2) 配置 Device 作为 PPPoE Server

配置虚拟模板参数，采用 PAP 认证对端，配置本端 IP 地址，并使用 PPP 地址池为对端分配 IP 地址。

```
<Device> system-view
[Device] interface virtual-template 1
[Device-Virtual-Template1] ppp authentication-mode pap domain system
[Device-Virtual-Template1] remote address pool 1
[Device-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[Device-Virtual-Template1] quit
```

配置 PPP 地址池，包含 9 个可分配的 IP 地址。

```
[Device] ip pool 1 1.1.1.2 1.1.1.10
```

在 Virtual-Ethernet 接口上使能 PPPoE Server。

```
[Device] interface virtual-ethernet 1
[Device-Virtual-Ethernet1] mac-address 0001-0000-0001
[Device-Virtual-Ethernet1] pppoe-server bind virtual-template 1
[Device-Virtual-Ethernet1] quit
```

对 ATM 接口进行配置。

```
[Device] interface atm 2/4/0.1
[Device-ATM2/4/0.1] pvc to_adsl_a 0/60
[Device-ATM2/4/0.1-pvc-to_adsl_a-0/60] map bridge virtual-ethernet 1
[Device-ATM2/4/0.1-pvc-to_adsl_a-0/60] quit
[Device-ATM2/4/0.1] quit
```

在系统缺省的 ISP 域 system 下，配置域用户使用 RADIUS 认证/授权/计费方案。

```
[Device] domain system
[Device-isp-system] authentication ppp radius-scheme cams
[Device-isp-system] authorization ppp radius-scheme cams
[Device-isp-system] accounting ppp radius-scheme cams
[Device-isp-system] quit
```

配置 RADIUS 方案以及 RADIUS 认证/授权/计费服务器的 IP 地址和端口号。

```
[Device] radius scheme cams
[Device-radius-cams] primary authentication 11.110.91.146 1812
[Device-radius-cams] primary accounting 11.110.91.146 1813
```

配置与 RADIUS 服务器交互报文时使用的认证、计费共享密钥为明文 expert。

```
[Device-radius-cams] key authentication simple expert
[Device-radius-cams] key accounting simple expert
[Device-radius-cams] quit
```

(3) 配置 RADIUS 服务器

在 RADIUS 服务器上配置认证与计费的共享密钥 expert。

在 RADIUS 服务器上增加一个 PPPoE 用户，用户名为 user1，密码为 123456。

具体配置过程请参考实际使用的 RADIUS 服务器的用户手册。

4. 验证配置

配置完成后，AC 就可以与远端的 Device 建立 PPPoE 会话。

```
[AC] display pppoe-client session summary
Bundle ID    Interface    VA          RemoteMAC      LocalMAC       State
1      1     GE1/0/5      VA0         0001-0000-0001 00e0-1500-4100 SESSION
```

Host A、Host B、Host C 可以访问 Internet，比如通过 IE 打开网页等。