第 4 章　WAN 接入配置与管理

4.1 PPP 协议基础

PPP（Point to Point Protocol）协议是在点到点链路上承载网络层数据包的一种链路层协议。由于它能够提供用户认证、易于扩充，并且支持同/异步通信，因而获得了广泛应用。在普通 Modem 拨号，以及现在主流的 PPPoE 或 PPPoA ADSL，或者 Cable Modem WAN 接入中都要用到 PPP 协议。在路由器中的串行接口默认运行的就是 PPP 协议，不过一般情况下不需要对串行接口进行额外的配置。

4.1.1 PPP 协议体系结构

PPP 协议作为一种提供在点到点链路上的封装、传输网络层数据包的数据链路层协议，处于 OSI 参考模型的第二层（即数据链路层），主要被设计用来在支持全双工的异步链路上进行点到点之间的数据传输，为在点对点连接上传输多协议数据包提供了一个标准方法。不同于 X.25（一种分组交换协议）、Frame Relay（FR，帧中继）等数据链路层协议。

同时，PPP 又是一个多协议成帧机制，适合于在调制解调器、HDLC（Hight Data Link Control，高级数据链路控制）比特序列线路、SONET（Synchronous Optical Network，同步光纤网）和其他网络的物理层上使用。

PPP 协议由层次结构组成，如图 4-1 所示。PPP 通过使用底层（物理层）的功能，可以使用同步物理介质（如 ISDN、FR）或异步电路（如拨号连接）。PPP 的高层功能是利用其 NCP 协议族在多个网络层协议之间传递数据包。

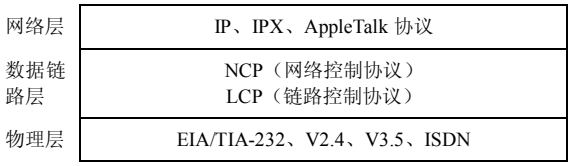

图 4-1 PPP 协议体系结构

PPP 高层协议包括 BCP（Bridge Control Protocol，网桥控制协议）、IPCP（Internet Protocol Control Protocol，IP 控制协议）、IPXCP（Internetwork Prcket Exchange Control Protocol，IPX 控制协议），更好地支持了网络层协议。在 PPP 的帧中，包含一些功能域，在这些域中用一些标准代码标识 PPP 封装的是什么网络层协议。

PPP 协议本身主要由封装、链路控制协议（LCP）、网络控制协议族（NCPs）和用于网络安全方面的认证协议族（PAP 和 CHAP）组成。PPP 协议的具体功能就是由这些协议提供支持的，具体体现在如下几个方面：

- 多协议数据报封装：PPP 封装提供了不同网络层协议同时在同一链路传输的多路复用技术。PPP 封装可保持对大多数常用硬件的兼容性。
- 链路控制（LC）：PPP 提供的 LCP（链路控制协议）功能全面，适用于大多数环境。LCP 具有就封装格式选项自动达成一致、处理数据包大小限制、探测环路链路和其他普通的配置错误、认证链路中对等单元的身份、决定链路功能正常或链路失败情况、终止链路等功能。
- 网络控制（NC）：PPP 协议中的 NCP（网络控制协议）是一种扩展链路控制协议，可用于

建立、配置、测试和管理数据链路连接。

- 网络安全认证：PPP 协议中的网络安全协议族（包括 PAP 和 CHAP）可用于为网络点对点连接提供身份认证，确保连接安全。

4.1.2　PPP 会话身份认证原理

在 PPP 的点对点通信中，可以采用 PAP 或 CHAP 身份认证方式（首选 CHAP 方式）对连接用户进行身份认证，以防非法用户的 PPP 连接。但这些认证是可选的，而不是必须的。如果需要认证，则发生在网络层协议配置之前，在链路层建立完成并且选择了认证协议后，通信双方就可以被认证了。在认证阶段中，要求链路发起方在认证选项中填写认证信息，以便确认用户得到了网络管理员的许可。在认证过程中，通信双方对等的路由器要彼此交换认证信息。

如果是采用 PAP 协议，则整个身份认证过程是两次握手认证过程，口令以明文传送。PAP 认证过程如图 4-2 所示。

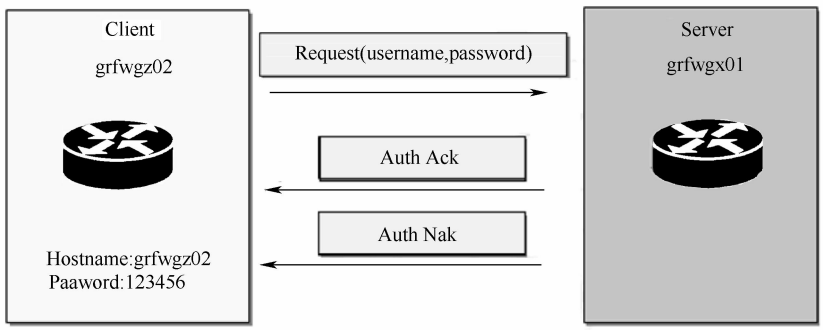

图 4-2　PAP 身份认证的两次握手

用文字描述如下：

（1）被认证方发送用户名和口令到认证方，示例中是以客户（Client）端 grfwgz02 向服务器（Server）端 grfwgz01 请求身份认证。

（2）认证方 grfwgz01 根据自己的网络用户配置信息查看是否有此用户及口令是否正确，然后返回不同的响应（Acknowledge 或 Not Acknowledge）。

（3）如果正确，则会给对端发送 ACK（应答确认）报文，通知对端已被允许进入下一阶段协商；否则发送 NCK（不确认）报文，通知对方认证失败。但此时并不会直接将链路关闭，客户端还可以继续尝试新的用户密码。只有当认证不通过次数达到一定值（默认为 4）时才会关闭链路，来防止因误传、网络干扰等造成不必要的 LCP 重新协商过程。

PAP 并不是一个健全的认证协议。它的特点是，在网络上以明文的方式传递用户名及口令，如在传输过程中被截获，便有可能对网络安全造成极大的威胁。因此它并不是一种强有效的认证方法，其密码以文本格式在电路上进行发送，对于窃听、重放或重复尝试和错误攻击没有任何保护，仅适用于对网络安全要求相对较低的环境。

如果采取 CHAP 协议进行身份认证，则需要三次握手认证协议，不直接发送口令，由主认证方首先发起认证请求。CHAP 的安全性比 PAP 高。CHAP 身份认证的三次握手流程如图 4-3 所示。用文字描述如下（同样以客户端 grfwgz02 向服务器端 grfwgz01 发送认证请求为例进行介绍）：

（1）当客户端要求与认证服务器连接时，并不是像 PAP 认证方式那样直接由客户端输入用户名和密码，而首先由认证方 grfwgz01 向被认证方 grfwgz02 发送一个作为身份认证请求的随机产生的报文，并同时将自己配置用于认证的主机名（或用户名）附带上一起发送给被认证方。

（2）被认证方得到认证方的认证请求（Challenge）后，便根据此报文中认证方的主机名（或

用户名）和自己的用户表查找对应用户账户口令。如在用户表中找到与认证方主机名（或用户名）相同的用户账户，便利用接收到的随机报文和该用户的密匙以 Md5 算法生成应答（Response），随后将应答和自己用于认证的主机名（或用户名）发送给认证服务器。

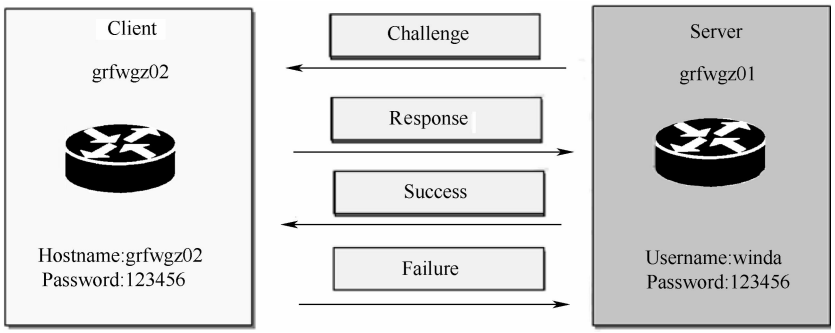

图 4-3　CHAP 身份认证的三次握手

（3）认证方接到此应答后，再利用对方的主机名（用户名）在自己的用户表中查找自己系统中保留的口令字，找到后再用自己的保留口令字（密匙）和随机报文以 Md5 算法生成结果，与被认证方应答比较。认证成功认证服务器会发送一条 ACK 报文（Success），否则会发送一条 NAK 报文（Failure）。

CHAP 身份认证的特点是只在网络上传输用户名，而并不以明文方式直接传输用户账户口令，因此它的安全性比 PAP 要高。CHAP 认证方式使用不同的询问消息，每个消息都是不可能预测的唯一值，这样就可以防范再生攻击。不断询问可以被限制在一次攻击中的时间内，本地路由器可以控制询问的频率和时间。

4.2　PPP 协议配置

路由器上的同/异步串行接口（Serial）默认封装的都是 PPP 协议，与对方的连接都是采用点对点方式，所以默认情况下都是需要对接口上的 PPP 协议进行配置。当然并不是所有串口都要求全面配置 PPP 协议，如大多数情况下是无需配置 PPP 会话认证的，所以一般情况下，串口都可以在没有任何专门配置的情况下使用。仅在需要在直接连接的双方串行接口间采用 PPP 会话认证、PPP 参数和 IP 地址协商等功能时才需要进行配置。

4.2.1　PPP 协议配置基本思路

在配置 H3C 路由器的 PPP 会话过程中，整个 PPP 协议的基本配置（不介绍太复杂的配置）思路如表 4-1 所示，主要包括 PPP 协议封装、PPP 会话认证、PPP 协商参数等几个方面的配置。从中可以看出，里面没有一项是必须配置的，均为可选。

表 4-1　PPP 的基本配置思路

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> system-view	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] interface serial 2/0	进入指定接口的视图

续表

步骤	命令	说明
Step 3	**link-protocol ppp** 例如： [Sysname-Serial2/0] link-protocol ppp	（可选）配置接口封装的链路层协议为 PPP。默认接口封装的链路层协议为 PPP
Step 4	**timer hold** *seconds* 例如： [Sysname-Serial2/0] **timer hold** 20	（可选）配置轮询时间间隔。默认轮询时间间隔为 10 秒
Step 5	配置 PPP PAP 会话认证，参见 4.2.2 节	（二者可选其一）默认 PPP 不进行认证
	配置 PPP CHAP 会话认证，参见 4.2.3 和 4.2.4 节	
Step 6	配置 PPP 协商参数，参见 4.3 节	（可选）配置 PPP 协商参数，一般不需要配置

1．link-protocol ppp 命令

link-protocol ppp 接口视图命令用来配置接口封装的链路层协议为 PPP。默认除以太网接口外，其他接口封装的链路层协议均为 PPP。所以，除以太网接口外，其他接口如果要使用 PPP 封装的话，可以不配置此命令。

以下示例是配置接口 Serial2/0 封装的链路层协议为 PPP。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol ppp
```

2．timer hold 命令

timer hold *seconds* 接口视图命令用来配置轮询时间间隔，轮询时间间隔指的是接口发送 keepalive 报文的周期。参数 *seconds* 用来指定接口发送 keepalive 报文的周期，取值范围为 0～32767，单位为秒。如果将轮询时间间隔配置为 0 秒，则不发送 keepalive 报文。

默认轮询时间间隔为 10 秒，可用 **undo timer hold** 命令恢复默认情况。

在速率非常低的链路上，参数 *seconds* 不能配置得过小。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。而接口如果在多个 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了故障。

当接口配置了 PPP 时，链路两端设备配置的轮询时间间隔必须相等。

以下示例是配置接口 Serial2/0 的轮询时间间隔为 20 秒。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] timer hold 20
```

4.2.2　配置 PAP 认证

PPP 有两种认证方式：PAP 为两次握手认证，由被认证方发起，密码为明文；CHAP 为三次握手认证，由认证方发起，密码为密文。但无论是 CHAP 还是 PAP 都只是一个认证过程，最终能否通过认证还需要 AAA 来作决定（当然这仅是在配置了 AAA 认证的情况下）。AAA 可利用本地认证数据库认证或由 AAA 服务器进行认证。本节介绍的是 PAP 认证方式的配置步骤。

对于拨号接口的认证，建议在物理接口和 Dialer（拨号）接口上都进行配置。因为当物理接口接收到 DCC 呼叫请求时，首先进行 PPP 协商并认证拨入用户的合法性，然后再将呼叫转交给上层协议进行处理。

1．认证方的 PAP 认证配置

在 PAP PPP 会话认证配置中，主要的配置是在认证方（相当于 PPP 服务器端），包括：认证模式、PAP 认证域、本地用于认证的用户账户和密码、本地用户的服务类型、本地认证方案，具体配置步骤如表 4-2 所示。

表 4-2　认证方的 PAP 认证配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 3	**ppp authentication-mode pap** [[**call-in**] **domain** *isp-name*] 例如： [Sysname-Serial2/0] **ppp authentication-mode pap domain** system	配置本地认证对端的方式为 PAP。默认 PPP 协议不进行认证
Step 4	**quit** 例如： [Sysname-Serial2/0] **quit**	退回系统视图
Step 5	**local-user** *username* 例如： [Sysname] **local-user** user1	创建用于认证对方的本地用户（也就是对方进行认证时所用的用户名），并进入本地用户视图
Step 6	**password** { **cipher** | **simple** } *password* 例如： [Sysname-luser-user1] **password simple** 123456	设置本地用户的密码
Step 7	**service-type ppp** 例如： [Sysname-luser-user1] **service-type ppp**	设置本地用户的服务类型为 PPP
Step 8	**quit** 例如： [Sysname-luser-user1] **quit**	退回系统视图
Step 9	**domain** *isp-name* 例如： [Sysname] **domain** test	（可选）创建一个 ISP 域，或者进入已创建 ISP 域的视图
Step 10	**authentication ppp local** 例如： [Sysname-isp-system]**authorization ppp local**	（可选）配置域用户使用本地认证方案

在以上配置步骤中，涉及到几个有关 PAP 认证的命令，下面具体介绍。

（1）ppp authentication-mode 命令。

ppp authentication-mode pap [[**call-in**] **domain** *isp-name*]命令是 **ppp authentication-mode** { **chap** | **pap** } [[**call-in**] **domain** *isp-name*] 接口视图命令的子命令，选择了专用于 PAP 认证的选项。它是用来配置本端 PPP 协议对对端设备的认证方式的。命令中的参数和选项说明如下：

- **chap**：二选一选项，指定采用 CHAP 认证方式。
- **pap**：二选一选项，指定采用 PAP 认证方式。
- **call-in**：可选项，表示只在远端用户呼入时才认证对方。
- **domain** *isp-name*：可选项，指定用户认证采用的域名，为 1～24 个字符的字符串。

默认 PPP 协议不进行认证，可用 **undo ppp authentication-mode** 命令取消配置的认证方式，即不进行认证。

【注意】如果配置时使用了域名（由 **domain** *isp-name* 可选项和参数对指定），则使用指定域进行认证，地址分配必须使用该域下配置的地址池（可通过 **display domain** 命令查看该域的配置）。如果配置时没有配置域，则判断用户名中是否带有 domain 信息。如果用户名中带有域信息，则以

用户名中的域为准（若该域名不存在，则认证被拒绝）；如果用户名中不带域，则使用系统默认的域（默认域可以通过 **domain default enable** 系统视图命令配置，若不配置，则默认域为 system）。

以下示例是设置在接口 Serial2/0 上采用 PAP 方法认证对端设备。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp authentication-mode pap domain system
```

（2）local-user 命令。

local-user *user-name* 系统视图命令用来添加用于本地 PPP 会话的用户账户，并进入本地用户视图。参数 *user-name* 用来指定要删除的本地 PPP 用户名，为 1～55 个字符的字符串，区分大小写。用户名不要携带域名，不能包括符号\、|、/、:、*、?、<、>和@，**且不能为 a、al 或 all**。

默认无本地 PPP 用户，可用 **undo local-user** *user-name* 命令删除指定的本地用户。

以下示例是添加名称为 winda 的本地 PPP 用户。

```
<Sysname> system-view
[Sysname] local-user winda
[Sysname-luser-user1]
```

（3）password 命令。

password { **cipher** | **simple** } *password* 本地用户视图命令用来设置本地 PPP 用户的密码。命令中的参数和选项说明如下：

- **cipher**：二选一选项，指定以密文方式显示密码。
- **simple**：二选一选项，指定以明文方式显示密码。
- *password*：指定设置的密码。明文密码可以是长度小于等于 63 位的连续字符串，密文密码的长度取值为 24 或 88 位。对于 **simple** 方式，必须是明文密码；对于 **cipher** 方式，可以是密文密码也可以是明文密码。

默认是没有配置本地 PPP 用户密码的，可用 **undo password** 命令取消本地用户的密码。

【注意】当采用 **local-user password-display-mode cipher-force** 命令后，即使用户通过 **password** 命令指定密码显示方式为明文显示（即 **simple** 方式），密码也会显示为密文。在 **cipher** 方式下，长度小于等于 16 的明文密码会被加密为长度是 24 的密文，长度大于 16 且小于等于 63 的明文密码会被加密为长度是 88 的密文。当用户输入长度为 24 的密码时，如果密码能够被系统解密，则按密文密码处理；若不能被解密，则按明文密码处理。

以下示例是设置名称为 winda 的密码为明文显示，密码为 123456。

```
<Sysname> system-view
[Sysname] local-user winda
[Sysname-luser-user1] password simple 123456
```

（4）service-type 命令。

service-type ppp 本地用户视图命令用来设置用户可以使用的服务类型为 PPP。

默认系统不对用户授权任何服务，可用 **undo service-type ppp** 命令删除用户可以使用的 PPP 服务类型。

以下示例是指定用户 user1 可以使用 PPP 服务。

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type PPP
```

（5）domain 命令。

domain *isp-name* 系统视图命令用来创建 ISP 域并进入其视图。参数 *isp-name* 用来指定要创建的 ISP 域名，为 1～24 个字符的字符串，不区分大小写，不能包括/、:、*、?、<、>、@等字符。需要注意的是，使用此命令时，如果指定的 ISP 域不存在，系统将会创建一个新的 ISP 域，所有的 ISP 域在创建后即处于 **active** 状态。另外，系统中默认存在的 ISP 域 system 不能被删除，

只能修改。

默认系统存在一个名称为 system 的 ISP 域，可用 **undo domain** 命令删除指定的 ISP 域。

以下示例是创建一个新的 ISP 域 test，并进入其视图。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test]
```

（6）authorization ppp 命令。

authentication ppp local ISP 域视图命令用来为 PPP 用户配置本地授权方案。需要注意的是，当前 ISP 域所引用的 RADIUS 或 HWTACACS 方案必须是已配置的；RADIUS 授权是特殊的流程，只是在认证和授权的 RADIUS 方案相同的条件下 RADIUS 授权起作用，否则授权失败。

默认 PPP 用户采用默认的授权方案，可用 **undo authorization ppp** 命令恢复默认情况。

以下示例是设置在系统默认的 ISP 域 system 下为 PPP 用户配置本地授权认证方案。

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]authorization ppp local
```

2．被认证方的 PAP 认证配置

在 PAP 认证过程中，被认证方（相当于 PPP 客户端）的配置很简单，只需要在对应的串口下配置所使用的本地 PAP 认证用户账户和密码即可，所使用的命令是 **ppp pap local-user** *username* **password** { **cipher** | **simple** } *password* 接口视图命令。命令中的参数和选项说明如下：

- *username*：本地设备被向采用 PAP 认证方式的对端设备发送的用户名，为 1～80 个字符的字符串。
- **simple**：二选一选项，指定采用明文密码显示方式。
- **cipher**：二选一选项，指定采用密文密码显示方式。
- *password*：本地设备被向采用 PAP 认证方式的对端设备发送的密码，为 1～48 个字符。对于 **simple** 方式，必须是明文密码；对于 **cipher** 方式，可以是密文密码，也可以是明文密码。明文密码可以是长度小于等于 48 的连续字符串，密文密码的长度必须是 24 位或 64 位。

所配置的用户名和密码必须与在认证方配置的本地用户名和密码一致，参见表 4-2 所示的配置步骤。

默认被对端以 PAP 方式认证时，本地设备发送的用户名和密码均为空，不进行认证，可用 **undo ppp pap local-user** 命令取消配置的用户名和密码。

以下示例是配置本地设备被对端以 PAP 方式认证时发送的用户名为 winda，密码为 123456。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp pap local-user winda password simple 123456
```

4.2.3 认证方配置了用户名情形下的 CHAP 认证配置

在本章前面已经介绍了，PPP 会话 CHAP 认证分为认证方配置了认证用户名和认证方没有配置认证用户名两种情况，所以在此也要分两种情形来介绍。本节先介绍认证方配置了执行认证用户名的情形下的 CHAP 认证配置方法。同样需要同时配置认证方和被认证方。

1．认证方 CHAP 配置

在认证方配置了认证用户名的情形下，认证方的 CHAP 认证配置步骤如表 4-3 所示。对比前面 PAP 认证过程中的认证方配置步骤可以看出，两者非常类似，都是配置认证模式、本地认证用户和

密码、本地用户的服务类型和本地认证方案。所不同的是认证模式的选择上，此处选择的是CHAP，而上节选择的是 PAP。

表 4-3　认证方配置了认证用户名时的认证方 CHAP 认证的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 3	**ppp authentication-mode chap** [[**call-in**] **domain** *isp-name*] 例如： [Sysname-Serial2/0] **ppp authentication-mode chap domain** test	配置本地认证对端的方式为 CHAP。默认 PPP 协议不进行认证
Step 4	**ppp chap user** *username* 例如： [Sysname-Serial2/0] **ppp chap user** Root	配置采用 CHAP 认证时认证方的用户名，必须与在被认证方通过 **local-user** *username* 命令创建的本地用户名一致
Step 5	**quit** 例如： [Sysname-Serial2/0] **quit**	退回系统视图
Step 6	**local-user** *username* 例如： [Sysname] **local-user** user1	创建用于被认证方认证的本地用户，并进入本地用户视图。这里所创建的用户要与被认证方通过 **ppp chap user** *username* 命令配置的认证用户名一致
Step 7	**password** { **cipher** | **simple** } *password* 例如： [Sysname-luser-user1] **password simple** 123456	设置本地用户的密码
Step 8	**service-type ppp** 例如： [Sysname-luser-user1] **service-type ppp**	设置本地用户的服务类型为 PPP
Step 9	**quit** 例如： [Sysname-luser-user1] **quit**	退回系统视图
Step 10	**domain** *isp-name* 例如： [Sysname] **domain** test	（可选）创建一个 ISP 域，或者进入已创建 ISP 域的视图
Step 11	**authentication ppp local** 例如： [Sysname-isp-system]**authorization ppp local**	（可选）配置域用户使用本地认证方案

另外，在 CHAP 认证中是通过 **ppp chap user** *username* 命令配置本端用于 CHAP 认证的用户名（但这个用户是在对端数据库中存在的），以取代在 PAP 认证时被认证方中配置的 **ppp pap local-user** *username* **password** { **cipher** | **simple** } *password* 命令。除此之外，所有配置命令均与上节的认证方式配置命令一样，因此不再赘述。

ppp chap user *username* 命令用来配置本端用于 CHAP 认证的用户名。参数 *username* 用来配置 CHAP 认证的用户名，为 1～80 个字符，该用户名是发送到被认证方进行 CHAP 认证时使用的用户名。指出只有该用户才可以访问认证方（PPP 服务器）。该命令配置的用户名一定要与被认证方通过 **local-user** *username* 命令配置的本地用户名一致。

默认 CHAP 认证的用户名为空，也就是认证方不对被认证方进行认证，可用 **undo ppp chap user** 命令删除已有的配置。

以下示例是配置接口 Serial2/0 进行 CHAP 认证时的用户名为 lycb。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp chap user lycb
```

2．被认证方的 CHAP 认证配置

在认证方配置了认证的用户名的情形下，被认证方的 CHAP 认证配置也是要注意使用 **ppp chap user** *username* 命令配置的认证用户账户要与认证方使用 **local-user** *username* 命令配置的本地用户名一致，具体的配置步骤如表 4-4 所示。因为这里的配置命令在本章前面都已做了详细介绍，所以在此不再赘述。

表 4-4　认证方配置了认证用户名时的被认证方 CHAP 认证的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/1	进入指定接口的视图
Step 3	**ppp chap user** *username* 例如： [Sysname-Serial2/1] **ppp chap user** user1	配置采用 CHAP 认证时被认证方的用户名。在认证方上使用 **local-user** *username* 命令为被认证方配置的本地用户的用户名必须跟此处配置的一致
Step 4	**quit** 例如： [Sysname-Serial2/1] **quit**	退回系统视图
Step 5	**local-user** *username* 例如： [Sysname] **local-user** Root	为认证方创建本地用户，并进入本地用户视图。这里所创建的用户要与认证方使用 **ppp chap user** *username* 命令配置的用户名和密码一样
Step 6	**password** { **cipher** | **simple** } *password* 例如： [Sysname-luser-user1] **password simple** 654321	为认证方设置本地用户的密码。这里所配置的密码要与认证方使用 **ppp chap user** *username* 命令配置的用户账户的密码一样

4.2.4　认证方没有配置用户名情形下的 CHAP 认证配置

认证方没有配置用户名也就是没有通过 **ppp chap user** *username* 命令配置进行 CHAP 认证的用户名。此时只需要在认证方使用 **local-user** *username* 命令配置本地认证的用户名和密码。但在被认证方要使用 **ppp chap user** *username* 命令配置进行 CHAP 认证的用户名，它与认证方使用 **local-user** *username* 命令配置的本地用户一致，但无须使用 **local-user** *username* 命令配置本地用户，因为认证方不用使用 **ppp chap user** *username* 命令配置进行 CHAP 认证的用户。另外，在被认证方还要通过 **ppp chap password** { **cipher** | **simple** } *password* 命令配置认证用户的密码。

在认证方没有配置认证用户名的情况下，认证方的 CHAP 认证配置步骤如表 4-5 所示，被认证方的 CHAP 认证配置步骤如表 4-6 所示。

表 4-5　认证方没有配置认证用户名时的认证方 CHAP 认证的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 3	**ppp authentication-mode chap** [[**call-in**] **domain** *isp-name*] 例如： [Sysname-Serial2/0] **ppp authentication-mode chap domain** test	配置本地认证对端的方式为 CHAP。默认 PPP 协议不进行认证
Step 4	**quit** 例如： [Sysname-Serial2/0] **quit**	退回系统视图

续表

步骤	命令	说明
Step 5	**local-user** *username* 例如： [Sysname] **local-user** user1	为被认证方创建本地用户，并进入本地用户视图
Step 6	**password** { **cipher** | **simple** } *password* 例如： [Sysname-luser-user1] **password simple** 123456	设置本地用户的密码
Step 7	**service-type ppp** 例如： [Sysname-luser-user1] **service-type ppp**	设置本地用户的服务类型为 PPP
Step 8	**quit** 例如： [Sysname-luser-user1] **quit**	退回系统视图
Step 9	**domain** *isp-name* 例如： [Sysname] **domain** test	创建一个 ISP 域，或者进入已创建 ISP 域的视图
Step 10	**authentication ppp local** 例如： [Sysname] **authentication ppp local**	（可选）配置域用户使用本地认证方案

表 4-6　认证方没有配置认证用户名时的被认证方 CHAP 认证的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/1	进入指定接口的视图
Step 3	**ppp chap user** *username* 例如： [Sysname-Serial2/1] **ppp chap user** user1	配置采用 CHAP 认证时被认证方的用户名。在认证方上使用 **local-user** *username* 命令为被认证方配置的本地用户的用户名必须跟此处配置的一致
Step 4	**ppp chap password** { **cipher** | **simple** } *password* 例如： [Sysname-Serial2/1] **ppp chap password simple** 123456	设置默认的 CHAP 认证密码。这里配置的密码一定要与认证方使用 **local-user** *username* 命令配置的本地用户账户密码一样

上述配置步骤中，除了被认证方配置 CHAP 认证用户密码的 **ppp chap password** { **cipher** | **simple** } *password* 接口视图命令外，其他均已在本章前面介绍，不再赘述。**ppp chap password** { **cipher** | **simple** } *password* 接口视图命令用来配置进行 CHAP 认证时采用的默认密码。可用 **undo ppp chap password** 命令取消配置的密码。命令中的参数和选项说明如下：

- **cipher**：二选一选项，指定采用密文方式显示密码。
- **simple**：二选一选项，指定采用明文方式显示密码。
- *password*：CHAP 认证的默认密码，为 1～48 个字符的字符串。对于 **simple** 方式，必须是明文密码；对于 **cipher** 方式，可以是密文密码也可以是明文密码。明文密码可以是长度小于等于 48 的连续字符串，密文密码的长度必须是 24 位或 64 位。

以下示例是配置本地设备以 CHAP 方式被对端设备认证时，默认密码为 sysname 且为明文显示。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp chap password simple sysname
```

4.2.5　PPP PAP 单向认证配置示例

单向认证是指只由一方对另一方进行认证，这样只要求在认证方配置有被认证方所发送的认证

用户账户即可，当然还要在认证方配置 PAP 本地认证方式。本示例的拓扑结构如图 4-4 所示，Router A 和 Router B 之间用接口 Serial2/0 互连，仅要求 Router A 用 PAP 方式认证 Router B，Router B 不需要对 Router A 进行认证。

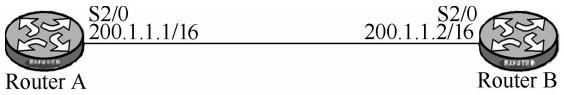

图 4-4　PPP 会话 PAP 认证配置示例拓扑结构

具体的配置步骤如下：

（1）Router A 的配置。

1）在本地用户视图中创建用于 PPP 会话 PAP 认证的本地用户 userb，以便对方（Router B）在输入认证用户时在本地（Router A）用户数据库中可以查到。

```
<RouterA> system-view
[RouterA] local-user userb
```

2）设置本地用户 userb 的简单密码为 passb。

```
[RouterA-luser-userb] password simple passb
```

3）设置本地用户 userb 的服务类型为 PPP。

```
[RouterA-luser-userb] service-type ppp
```

4）配置与 Router B 相连的 PPP 接口 serial 2/0 封装 PPP 链路层协议。

```
[RouterA-luser-userb] quit
[RouterA] interface serial 2/0
[RouterA-Serial2/0] link-protocol ppp
```

5）配置本地认证 Router B 的方式为 PAP，域名采用系统默认的 system。

```
[RouterA-Serial2/0] ppp authentication-mode pap domain system
```

6）配置 Router A 的 serial 2/0 接口的 IP 地址为 200.1.1.1 255.255.0.0。

```
[RouterA-Serial2/0] ip address 200.1.1.1 16
[RouterA-Serial2/0] quit
```

7）指定 ISP 域为默认的 system 域。

```
[RouterA] domain system
```

8）配置域用户使用本地认证方案。

```
[RouterA-isp-system] authentication ppp local
```

（2）Router B 的配置。

1）配置与 Router A 相连的 serial 2/0 接口封装的链路层协议为 PPP。

```
<RouterB> system-view
[RouterB] interface serial 2/0
[RouterB-Serial2/0] link-protocol ppp
```

2）配置本地用于被 Router A 以 PAP 方式本地认证的 PAP 用户名和密码。必须与 Router A 上创建的本地用户账户名和密码完全一样。

```
[RouterB-Serial2/0] ppp pap local-user userb password simple passb
```

3）配置与 Router A 相连的 serial 2/0 接口的 IP 地址为 200.1.1.2 255.255.0.0。这个 IP 地址必须与 Router A 上 serial 2/0 接口的 IP 地址在同一网段。

```
[RouterB-Serial2/0] ip address 200.1.1.2 16
```

认证配置结果：可通过在被认证的 Router B 上执行 **display interface** serial 2/0 命令查看接口的物理层和链路层的状态和 PPP 链路层相关协议的状态来证明链路的 PPP 协商是否已经成功（注意输出信息中的粗体字部分），并且可通过执行 Ping 命令认证 Router A 和 Router B 可以互相 **ping** 通对方。执行以上两命令的输出示例如下：

```
[RouterB-Serial2/0] display interface serial 2/0
Serial2/0 current state: UP
Line protocol current state: UP
Description: Serial2/0 Interface
```

```
The Maximum Transmit Unit is 1500, Hold timer is 10（sec）
Internet Address is 200.1.1.2/16 Primary
Link layer protocol is PPP
LCP opened, IPCP opened
Output queue :  （Urgent queuing : Size/Length/Discards）    0/100/0
Output queue :  （Protocol queuing : Size/Length/Discards）    0/500/0
Output queue :  （FIFO queuing : Size/Length/Discards）    0/75/0
Interface is V35
      206 packets input,    2496 bytes
      206 packets output,    2492 bytes

[RouterB-Serial2/0] ping 200.1.1.1
  PING 200.1.1.1: 56    data bytes, press CTRL_C to break
    Reply from 200.1.1.1: bytes=56 Sequence=1 ttl=255 time=103 ms
    Reply from 200.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 200.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 200.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 200.1.1.1: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 200.1.1.1 ping statistics ---
    5 packet（s）  transmitted
    5 packet（s）  received
    0.00% packet loss
    round-trip min/avg/max = 1/23/103 ms
```

4.2.6　PPP PAP 双向认证配置示例

双向认证是指互连的双方要相互进行认证，要求双方在各自的**本地**用户视图中配置了**对方**进行 PAP 认证时所发送的用户账户，而且双方都要配置 PAP 本地认证方式。本示例的拓扑结构仍参见图 4-4，Router A 和 Router B 之间用接口 Serial2/0 互连，不过此时要求 Router A 和 Router B 用 PAP 方式相互认证对方。

具体配置步骤如下：

（1）Router A 的配置。

```
<RouterA> system-view
[RouterA] local-user userb
[RouterA-luser-userb] password simple passb
[RouterA-luser-userb] service-type ppp
[RouterA-luser-userb] quit
[RouterA] interface serial 2/0
[RouterA-Serial2/0] link-protocol ppp
[RouterA-Serial2/0] ppp authentication-mode pap domain system
[RouterA-Serial2/0] ppp pap local-user usera password simple passa  !---配置本地被 Router B 以 PAP 方式认证时 Router A 发送的 PAP
                                                                    !---用户名为 usera 和密码为 passa。因为这里要配置的是双向认证
[RouterA-Serial2/0] ip address 200.1.1.1 16
[RouterA-Serial2/0] quit
[RouterA] domain system
[RouterA-isp-system] authentication ppp local
```

对比上节的 Router A 配置可以看出，两者基本上一样，只是在上节 Router A 的第 5 步和第 6 步之间插入了一条配置 Router A 被 Router B PAP 认证的用户名和密码的 **ppp pap local-user** 命令配置用于向 Router B 发送 PAP 认证的用户名和密码。

（2）Router B 的配置。

因为是双向 PAP 认证，所以 Router B 的配置命令与 Router A 的基本一样，不同的只是所配置的具体参数值。具体如下：

```
<RouterB> system-view
[RouterB] local-user usera
[RouterB-luser-usera] password simple passa
```

```
[RouterB-luser-usera] service-type ppp
[RouterB-luser-usera] quit
[RouterB] interface serial 2/0
[RouterB-Serial2/0] link-protocol ppp
[RouterB-Serial2/0] ppp authentication-mode pap domain system
[RouterB-Serial2/0] ppp pap local-user userb password simple passb
[RouterB-Serial2/0] ip address 200.1.1.2 16
[RouterB-Serial2/0] quit
[RouterB] domain system
[RouterB-isp-system] authentication ppp local
```

同样可以前面提到的 **display interface** serial 2/0 和 **ping** 命令认证结果。

4.2.7 PPP CHAP 认证配置示例

本示例的拓扑结构仍参见图 4-4。要求设备 Router A 用 CHAP 方式认证设备 Router B，此时认证方为 Router A，被认证方为 Router B。这里要区分认证方是否配置用户名这两种情况进行配置。

1．认证方配置用户名时以 CHAP 方式认证对端的配置方法

这种情况下的配置步骤如下：

（1）Router A 的配置。

1）在本地用户视图中添加用于 PPP 会话 CHAP 认证的本地用户 userb，以便对方在输入认证用户时在本地用户数据库中可以查到，只有这样才能进行用户认证。

```
<RouterA> system-view
[RouterA] local-user userb
```

2）为对端设置本地用户 userb 的简单密码为 hello。

```
[RouterA-luser-userb] password simple hello
```

3）设置本地用户 userb 的服务类型为 PPP。

```
[RouterA-luser-userb] service-type ppp
```

4）配置与 Router B 相连的 PPP 接口 serial 2/0 封装 PPP 链路层协议。

```
[RouterA-luser-userb] quit
[RouterA] interface serial 2/0
[RouterA-Serial2/0] link-protocol ppp
```

5）配置采用 CHAP 认证时 Router A 的用户名为 usera。它要与对方（Router B）上用 **local-user** 命令配置的用户名和密码一样，是随质询报文一起发送到对端的认证用户名。

```
[RouterA-Serial2/0] ppp chap user usera
```

6）配置本地认证 Router B 的方式为 CHAP，域名采用系统默认的 system。

```
[RouterA-Serial2/0] ppp authentication-mode chap domain system
```

7）配置 Router A 的 serial 2/0 接口的 IP 地址为 200.1.1.1 255.255.0.0。

```
[RouterA-Serial2/0] ip address 200.1.1.1 16
[RouterA-Serial2/0] quit
```

8）创建名为 system 的 ISP 域。

```
[RouterA] domain system
```

9）配置域用户使用本地认证方案。

```
[RouterA-isp-system] authentication ppp local
```

（2）Router B 的配置。

Router B 的 CHAP 认证配置步骤与 Router A 的类似，只是不用配置本地认证方式，因为这里配置的是单向 CHAP 认证。但在 Router B 上要配置本地用户账户和密码，而且必须与 Router A 在使用 **ppp chap user** *username* 命令时所配置的用户账户名一样，当然密码也要求一样。

```
<RouterB> system-view
[RouterB] local-user usera   !---如果没有此命令，则本端不能认证对方是否有权力进行 CHAP 认证
[RouterB-luser-usera] password simple hello
```

```
[RouterB-luser-usera] service-type ppp
[RouterB-luser-usera] quit
[RouterB] interface serial 2/0
[RouterB-Serial2/0] link-protocol ppp
[RouterB-Serial2/0] ppp chap user userb    !---这是本端被认证方认证的用户名，与认证方通过 local-user 命令配置的本地用户名和
                                           !---密码一致
[RouterB-Serial2/0] ip address 200.1.1.2 16
```

2．认证方没有配置用户名时以 CHAP 方式认证对端的配置方法

在这种情况下，认证方 Router A 的配置与前面认证配置了用户名情况下的配置唯一区别就是没有使用 **ppp chap user** *username* 命令指定认证时的用户名。

```
<RouterA> system-view
[RouterA] local-user userb
[RouterA-luser-userb] password simple hello
[RouterA-luser-userb] service-type ppp
[RouterA-luser-userb] quit
[RouterA] interface serial 2/0
[RouterA-Serial2/0] ppp authentication-mode chap domain system
[RouterA-Serial2/0] ip address 200.1.1.1 16
[RouterA-Serial2/0] quit
[RouterA] domain system
[RouterA-isp-system] authentication ppp local
```

此时 Router B 的配置更简单了，只需要配置用于进行 CHAP 认证时所发送的本地用户名和密码，然后配置接口 IP 地址即可。具体如下：

（1）配置采用 CHAP 认证时 Router B 的用户名。

```
<RouterB> system-view
[RouterB] interface serial 2/0
[RouterB-Serial2/0] ppp chap user userb
```

（2）设置 userb 用户的 CHAP 认证密码。

```
[RouterB-Serial2/0] ppp chap password simple hello
```

（3）配置接口的 IP 地址。

```
[RouterB-Serial2/0] ip address 200.1.1.2 16
```

同样可以通过 **display interface** serial 2/0 命令查看接口的物理层和链路层状态，并且可以通过执行 **ping** 命令认证 Router A 和 Router B 可以互相 **ping** 通对方。

4.3　PPP 协商参数配置

本节所介绍的配置内容均为可选配置，主要介绍协商超时时间间隔、协商 IP 地址和协商 DNS 地址这三个方面常用的协商参数配置。其他还可以配置诸如 ACCM（Async-Control-Character-Maps，异步控制字符映射表）、ACFC（Address-and-Control-Field-Compression，地址控制字段压缩）和 PFC（Protocol-Field-Compression，协议字段压缩）协商参数，本节不作介绍。

4.3.1　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。超时时间间隔可选范围为 1～10 秒。具体配置步骤如表 4-7 所示。

在以上的配置步骤中，**ppp timer negotiate** *seconds* 接口视图配置命令用来配置 PPP 协商超时时间间隔。参数 *seconds* 用来指定协商超时时间间隔，取值范围为 1～10 秒。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。

表 4-7　协商超时时间间隔的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 3	**ppp timer negotiate** *seconds* 例如： [Sysname-Serial2/0] **ppp timer negotiate** 5	配置协商超时时间间隔。默认协商超时时间间隔为 3 秒

默认 PPP 协商超时时间间隔为 3 秒，可用 **undo ppp timer negotiate** 命令恢复默认情况。

以下示例是配置 PPP 协商超时时间间隔为 5 秒。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp timer negotiate 5
```

4.3.2　配置协商 IP 地址

在 PPP 会话中，协商 IP 地址的方式有两种：

- 配置路由器作为 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，可为本端接口配置 IP 地址协商属性，使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。该配置主要用于在通过 ISP 访问 Internet 时，得到由 ISP 分配的 IP 地址。
- 配置路由器作为 Server 端：若路由器是作为 Server 为对端设备分配 IP 地址，则应首先在域视图或系统视图下配置本地 IP 地址池，指明地址池的地址范围，然后在接口视图下指定该接口使用的地址池。

1．配置路由器作为客户端

如果路由器是作为 PPP 会话 Client 端，则 IP 地址的协商配置步骤如表 4-8 所示。

表 4-8　Client 端的 IP 地址协商配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 3	**ip address ppp-negotiate** 例如： [Sysname-Serial2/0] **ip address ppp-negotiate**	设置接口 IP 地址可协商属性

ip address ppp-negotiate 接口视图命令用来为本端接口配置 IP 地址可协商属性，使本端接口接受 PPP 协商产生的由对端分配的 IP 地址。

默认本端接口没有配置 IP 地址可协商属性，可用 **undo ip address ppp-negotiate** 命令取消为本端接口配置 IP 地址可协商属性。

以下示例是为接口 Serial2/0 配置 IP 地址可协商属性。

```
<Sysname> system-view
[Sysname] interface serial 2/0
```

```
[Sysname-Serial2/0] ip address ppp-negotiate
```

2．为不需要 PPP 认证的用户配置路由器作为服务器端

如果路由器是作为 PPP 会话服务器端，则进行 IP 地址协商时又要根据是否要进行 PPP 会话认证来区别配置。对于不需要进行认证的 PPP 用户，Server 端的配置方式如表 4-9 所示。

表 4-9　对于不需要进行认证的 PPP 用户的 Server 端 IP 地址协商的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**ip pool** *pool-number low-ip-address* [*high-ip-address*] 例如： [Sysname-isp-test] **ip pool** 0 129.102.0.1 129.102.0.10	定义 IP 地址池
Step 3	**interface** *interface-type interface-number* 例如： [Sysname] interface serial 2/0	进入要分配 IP 地址的接口
Step 4	**remote address pool** [*pool-number*] 或 **remote address** *ip-address* 例如： [Sysname-Serial2/0] **remote address pool**　0 或 [Sysname-Serial2/0] remote address 129.102.0.8	在接口上使用全局地址池给 PPP 用户分配 IP 地址，或者直接为对端指定 IP 地址。当配置了“**remote address pool**”命令，但没有指定地址池号时，默认使用 0 号全局地址池

（1）ip pool 命令。

ip pool *pool-number low-ip-address* [*high-ip-address*]系统视图/ISP 域视图命令用来定义为 PPP 用户分配 IP 地址的地址池。命令中的参数说明如下：

- *pool-number*：地址池编号，取值范围为 0～99。
- *low-ip-address* 和 *high-ip-address*：分别为地址池的起始和结束 IP 地址。一个地址池中起始 IP 地址和结束 IP 地址之间的地址数不能超过 1024。如果在定义 IP 地址池时不指定结束 IP 地址，则该地址池中只有一个 IP 地址，即起始 IP 地址。

在 ISP 域视图下，配置的 IP 地址池用于为相应的 ISP 域的 PPP 用户分配 IP 地址。这主要用于通过某接口接入的 PPP 用户较多，而接口所能分配的地址不够用的情况。例如，运行 PPPoE 协议的 Ethernet 接口最多可以接入 4096 个用户，但在该 Ethernet 接口的 Virtual Template 上只能配置一个地址池，而一个地址池最多只有 1024 个地址，这显然不能满足要求。通过配置 ISP 域的地址池可以为 ISP 的 PPP 用户分配地址，从而解决接口地址池中地址不够的问题。

默认没有定义为 PPP 用户分配 IP 地址的地址池，可用 **undo ip pool** 命令删除指定的 IP 地址池。

以下示例是配置 IP 地址池 0，地址范围为 129.102.0.1～129.102.0.10。

```
<Sysname> system-view
[Sysname-isp-test] ip pool 0 129.102.0.1 129.102.0.10
```

（2）remote address 命令。

remote address { *ip-address* | **pool** [*pool-number*] }接口视图命令用来配置为对端接口分配 IP 地址。其实它可以分成上述步骤中第 4 步中的两条命令。命令中的参数说明如下：

- *ip-address*：二选一参数，为对端分配的 IP 地址。
- **pool** [*pool-number*]：二选一参数，为对端分配 IP 地址使用的地址池。*pool-number* 用来指定地址池号，即将地址池 *pool-number* 中的一个 IP 地址分配给对端，取值范围为 0～99，默认值是 0。

当对端接口还未配置 IP 地址而本端设备已经有了 IP 地址时，可以配置本端设备为对端接口分配 IP 地址。这时，需要在对端设备上配置 **ip address ppp-negotiate** 命令，在本端设备上配置

remote address 命令，使对端接口接受由 PPP 协商产生分配的 IP 地址。

默认接口不为对端分配 IP 地址，可用 **undo remote address** 命令取消为对端接口分配 IP 地址。

【说明】该命令不具有地址分配的强制性，即在配置该命令后也允许对端自行配置 IP 地址；如果不希望（或不允许）对端自行配置 IP 地址，则必须再配置 **ppp ipcp remote-address forced** 命令，这将在本节后面介绍。

直接给对端分配 IP 地址或从全局地址池中给对端分配 IP 地址后，不能配置 **remote address** 和 **undo remote address** 命令了，只有当此 IP 地址被释放后才能进行配置，建议用户可以对此接口进行 **shutdown** 操作以释放 IP 地址，之后再执行这两条命令；通过 AAA 认证从指定域的地址池中给对端分配 IP 地址后，可以配置这两条命令，但是已经为对端分配的 IP 地址仍然可以正常使用，新的 PPP 接入采用新的配置分配 IP 地址。

该命令不即时生效，需要等到下一次 IPCP 协商时才会根据此配置进行协商。建议在配置此应用时先配置 **remote address** 命令，然后再配置 **ip address** 命令，使得配置能够生效。

以下示例是配置接口 Serial2/0 为对端分配的 IP 地址为 10.0.0.1。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] remote address 10.0.0.1
```

（3）为需要 PPP 认证的用户配置路由器作为 Server 端。

对于需要进行认证的 PPP 用户，Server 端的配置方式如表 4-10 所示，定义地址池所使用的域就是配置进行 PPP 认证时指定的域。

表 4-10　对于需要进行认证的 PPP 用户的 Server 端 IP 地址协商的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> system-view	进入系统视图
Step 2	**domain** *domain-name* 例如： [Sysname] **domain** test	进入指定的域视图
Step 3	**ip pool** *pool-number low-ip-address* [*high-ip-address*] 例如： [Sysname-isp-test] **ip pool** 0 129.102.0.1 129.102.0.10	定义域地址池
Step 4	**quit** 例如： [Sysname-isp-test] **quit**	退回系统视图
Step 5	**interface** *interface-type interface-number* 例如： [Sysname] interface serial 2/0	进入指定接口的视图
Step 6	**remote address pool** [*pool-number*] 例如： [Sysname-Serial2/0] **remote address pool** 0	使用域地址池给 PPP 用户分配 IP 地址。若配置该命令时不指定 *pool-number*，则在 IP 地址协商时依次使用该域下的地址池给用户分配 IP 地址
Step 7	**ppp ipcp remote-address forced** 例如： [Sysname-Serial2/0] **ppp ipcp remote-address forced**	（可选）配置 PPP IPCP 不允许对端使用自行配置的固定 IP 地址。默认 PPP IPCP 的 IP 地址协商情况为本端不具有地址分配的强制性，即设备本端允许对端自行配置地址。当对端明确请求本端分配地址时，本端给对端分配地址；若对端已自行配置 IP 地址时，本端不再强行给对端分配地址

以上配置步骤中，大多数命令均已在本章前面作了详细介绍，只有 **ppp ipcp remote-address forced** 接口视图命令没有介绍。它是用来使设备为对端分配 IP 地址时具有强制性，不允许对端使用自行配置的 IP 地址。

默认在 PPP 的 IPCP 协商阶段进行 IP 地址协商时，IP 地址协商情况为本端不具有地址分配的强制性，即本端设备允许对端自行配置 IP 地址。当对端明确请求本端分配 IP 地址时，本端给对端分配

IP 地址；若对端已自行配置 IP 地址时，本端不再强行给对端分配 IP 地址。可用 **undo ppp ipcp remote-address forced** 命令取消这种强制性，允许对端使用自行配置的 IP 地址。在不允许对端自行指定 IP 地址的情况下，设备本端接口下一定要配置 **ppp ipcp remote-address forced** 命令。

以下示例是设置接口 Serial2/0 准备为对端分配的 IP 地址为 10.0.0.1。此时，对端必须接收这个 IP 地址，不允许对端自行配置 IP 地址或不配置 IP 地址。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] remote address 10.0.0.1
[Sysname-Serial2/0] ppp ipcp remote-address forced
```

4.3.3　配置协商 DNS 服务器地址

路由器在进行 IP 地址协商的过程中可以进行 DNS 地址协商，此时路由器既可以被配置为 DNS 客户端，接收对端分配的 DNS 地址，也可以配置为 DNS 服务器端，为对端提供 DNS 地址。一般情况下，当 PC 与路由器通过 PPP 协议相连时，路由器应为 PC 机指定 DNS 地址，这样 PC 就可以通过域名直接访问 Internet；当路由器通过 PPP 协议连接运营商的接入服务器时，路由器应配置为被动接收或主动向 ISP 接入服务器请求 DNS 地址，这样路由器就可以使用接入服务器分配的 DNS 来解析域名。

当路由器担当 DNS 地址分配客户端时的配置步骤如表 4-11 所示。

表 4-11　路由器担当 DNS 地址分配客户端时的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 3	**ppp ipcp dns request** 例如： [Sysname-Serial2/0] **ppp ipcp dns request**	配置路由器主动请求对端指定 DNS 地址。默认禁止路由器主动向对端请求 DNS 服务器地址
Step 4	**ppp ipcp dns admit-any** 例如： [Sysname-Serial2/0] **ppp ipcp dns admit-any**	（可选）配置路由器被动地接收对端指定的 DNS 服务器地址。默认路由器不会被动地接收对端设备指定的 DNS 服务器的 IP 地址

1．ppp ipcp dns request 命令

ppp ipcp dns request 接口视图命令用来配置设备可以主动向对端请求 DNS 服务器地址。当路由器通过 PPP 协议与其他设备相连时（通常为路由器拨号连接运营商的接入服务器），通过协商，路由器可以主动请求对端指定 DNS 地址，这样设备就可以使用对端设备指定的 DNS 来解析域名。

默认禁止设备主动向对端请求 DNS 服务器地址，可用 **undo ppp ipcp dns request** 命令恢复默认情况。

以下示例是配置 Serial2/0 接口主动请求 DNS 服务器地址。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp ipcp dns request
```

2．ppp ipcp dns admit-any 命令

ppp ipcp dns admit-any 接口视图命令用来配置设备可以被动地接收对端设备指定的 DNS 服务器的 IP 地址，即设备不发送 DNS 请求也能接收对端设备分配的 DNS 服务器的 IP 地址。当路由器

通过 PPP 协议与其他设备相连时，通过协商，路由器可以被动地接收对端设备指定的 DNS 服务器地址，这样路由器就可以使用对端设备指定的 DNS 服务器来解析域名。

默认设备不会被动地接收对端设备指定的 DNS 服务器的 IP 地址，可用 **undo ppp ipcp dns admit-any** 命令禁止设备被动地接收对端设备指定的 DNS 服务器的 IP 地址。

【注意】在配置此命令之前必须配置 ppp ipcp dns request 命令。

以下示例是配置本地设备的 Serial2/0 接口可以被动地接收对端指定的 DNS 服务器地址。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp ipcp dns request
[Sysname-Serial2/0] ppp ipcp dns admit-any
```

如果要配置路由器为对端设备指定 DNS 服务器地址，则需要按如表 4-12 所示的步骤进行配置。

表 4-12　路由器担当 DNS 地址分配服务器端的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 3	**ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*] 例如： [Sysname-Serial2/0] **ppp ipcp dns** 100.1.1.1 100.1.1.2	使路由器为对端设备指定 DNS 服务器地址。默认路由器不为对端设备指定 DNS 服务器的 IP 地址

以上配置步骤中的 **ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]接口视图命令用来配置路由器为对端设备指定 DNS 服务器 IP 地址。参数 *primary-dns-address* 用来指定主 DNS 服务器的 IP 地址，参数 *secondary-dns-address* 用来指定从 DNS 服务器的 IP 地址。

当设备之间通过 PPP 协议相连时，通过协商，路由器可以为对端 PC 设备指定 DNS 服务器的 IP 地址（但需要等待对端请求，不会主动给对端指定 DNS 的地址）。这样，对端 PC 机就可以通过域名直接访问网络。如果 PC 与路由器通过 PPP 协议相连时，用户可以在 PC 上使用命令 **winipcfg** 或 **ipconfig /all** 来查看路由器为其提供的 DNS 服务器的 IP 地址。路由器可以为对端设备提供主 DNS 和从 DNS 两个服务器的 IP 地址。

默认设备不为对端设备指定 DNS 服务器的 IP 地址，可用 **undo ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]命令禁止设备为对端设备指定 DNS 服务器的 IP 地址。

以下示例是配置路由器为对端设备分配的主 DNS 服务器的 IP 地址为 100.1.1.1，从 DNS 服务器的 IP 地址为 100.1.1.2。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp ipcp dns 100.1.1.1 100.1.1.2
```

4.3.4　PPP 协商 IP 地址配置示例

本示例的网络拓扑结构如图 4-5 所示。Router A 通过 PPP 协商，为对端设备 Router B 的接口 Serial2/0 分配 IP 地址。

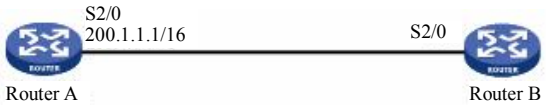

图 4-5　PPP 协商 IP 地址配置示例拓扑结构

具体的配置步骤如下：

（1）Router A 的配置。

1）创建用于为对端分配 IP 地址的本地 IP 地址池。

```
<RouterA> system-view
[RouterA] ip pool 1 200.1.1.10 200.1.1.20
```

2）配置接口 Serial2/0 的 IP 地址。

```
[RouterA] interface serial 2/0
[RouterA-Serial2/0] ip address 200.1.1.1 255.255.255.0
```

3）配置为对端接口在所创建的 IP 地址池中分配 IP 地址。

```
[RouterA-Serial2/0] remote address pool 1
```

（2）Router B 的配置。

1）在接口 Serial2/0 启用通过协商获取 IP 地址。

```
<RouterB> system-view
[RouterB] interface serial 2/0
[RouterB-Serial2/0] ip address ppp-negotiate
```

2）配置完成后，通过 **display brief interface** serial 2/0 命令查看接口 Serial2/0 的摘要信息。可以看到接口链路层协议已激活，并且已获得 IP 地址（注意输出信息中的粗体字部分）。

```
[RouterB-Serial2/0] display brief interface serial 2/0
The brief information of interface（s） under route mode:
Interface                 Link      Protocol-link   Protocol type     Main IP
S2/0                      UP        UP              PPP               200.1.1.10
```

3）此时可以通过 ping 命令认证配置结果，具体如下，证明可成功 ping 通了（注意输出信息中的粗体字部分）。

```
 [RouterB] ping 200.1.1.1
   PING 200.1.1.1: 56  data bytes, press CTRL_C to break
     Reply from 200.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
     Reply from 200.1.1.1: bytes=56 Sequence=2 ttl=255 time=4 ms
     Reply from 200.1.1.1: bytes=56 Sequence=3 ttl=255 time=4 ms
     Reply from 200.1.1.1: bytes=56 Sequence=4 ttl=255 time=10 ms
     Reply from 200.1.1.1: bytes=56 Sequence=5 ttl=255 time=4 ms

   --- 200.1.1.1 ping statistics ---
     5 packet（s） transmitted
     5 packet（s） received
     0.00% packet loss
     round-trip min/avg/max = 1/4/10 ms
```

4.4　MP 配置

MP（MultiLink PPP，多链路 PPP）可以将多个 PPP 链路捆绑使用，以增加链路带宽。MP 会将报文分片（小于最小分片包长时不分片）后，从 MP 链路下的多个 PPP 通道发送到 PPP 对端，对端将这些分片组装起来递给网络层。MP 的作用主要有：增加带宽、负载分担、备份、利用分片降低时延。这样可以大大提高点对点数据传输效率。

4.4.1　MP 的实现方式和协商过程

MP 能在任何支持 PPP 封装的接口下工作，如串口（Serial）、ISDN 的 BRI/PRI 接口等，也包括 PPPoX（PPPoE、PPPoA、PPPoFR 等）这类虚拟接口，建议用户尽可能将同一类的接口捆绑使用，不要将不同类的接口捆绑使用。

1．MP 的实现方式

MP 的配置主要有两种方式：

（1）通过虚拟模板（Virtual-Template，VT）接口，VT 是用于配置一个虚拟访问（Virtual Access，VA）接口的模板，将多个 PPP 链路捆绑成 MP 之后，需要创建一个 VA 接口与对端交换数据。此时，系统将选择一个 VT，以便动态地创建一个 VA。

（2）利用 MP-group 接口。MP-group 是多个物理接口绑定，然后通过 PPP 点到点协议和对端端口建立连接。

这两种配置方式的主要区别在于：

- VT 接口方式可以与认证相结合，也可以根据对端的用户名找到指定的虚拟模板接口，从而利用模板上的配置创建相应的捆绑（Bundle，系统中用 VT 通道来表示），以对应一条 MP 链路。
- 一个 VT 接口还可以派出若干个捆绑，每个捆绑对应一条 MP 链路。那么这样一来，从网络层来看，这若干条 MP 链路会形成一个点对多点的网络拓扑。为区分 VT 接口派生出的多个捆绑，需要指定捆绑方式，系统在虚拟模板接口视图下提供了 **ppp mp binding-mode** 命令来指定绑定方式，绑定方式有 **authentication**、**both**、**descriptor** 三种，默认是 **both**。**authentication** 是根据认证用户名捆绑，**descriptor** 是根据终端描述符捆绑（LCP 协商时，会协商出这个选项值），**both** 是要同时参考这两个值捆绑。
- MP-group 接口与虚拟模板接口相比则单纯许多，它是 MP 的专用接口，不能支持其他应用，也不能利用对端的用户名来指定捆绑，同时也不能派生多个捆绑。但正因为它的简单，导致了它的快速高效、配置简单、容易理解。

2．协商过程

MP 协商包括 LCP 和 NCP 两个协商过程。LCP 协商是首先进行的，除协商一般的 LCP 参数外，还认证对端接口是否也工作在 MP 方式下，如果两端工作方式不同，LCP 协商不成功。NCP 协商是在 LCP 协商成功后进行的，根据 MP-group 接口或指定虚拟接口模板的各项 NCP 参数（如 IP 地址等）进行 NCP 协商，但物理接口配置的 NCP 参数不起作用。NCP 协商通过后，即可建立 MP 链路。

4.4.2 通过虚拟模板接口配置 MP

当采用虚拟模板接口配置 MP 时，又可分为两种情况。一种情况是将物理接口与虚拟模板接口直接关联：通过 **ppp mp virtual-template** 命令将 PPP 物理链路直接绑定到指定的虚拟模板接口上。这时可以配置 PPP 会话认证，也可以不配置 PPP 会话认证。如果不配置认证，系统将通过对端的终端描述符捆绑出 MP 链路；如果配置了认证，系统将通过用户名和/或对端的终端描述符捆绑出 MP 链路。另一种情况是将用户名与虚拟模板接口关联：根据认证通过后的用户名查找相关联的虚拟模板接口，然后根据用户名和对端终端描述符捆绑出 MP 链路。这种方式需要在要绑定的接口下配置 **ppp mp** 命令，同时配置双向认证（CHAP 或 PAP），否则链路协商不通。

【注意】ppp mp 和 ppp mp virtual-template 命令互斥，即同一个接口只能配置成通过认证的绑定或直接绑定中的一种。而且，对于需要绑定在一起的接口，必须采用同样的配置方式。实际使用中也可以配置单向认证，即一端直接将物理接口绑定到虚拟模板接口，另一端则通过用户名查找虚拟模板接口。不推荐使用同一个虚拟模板接口配置多种业务（如 MP、L2TP、PPPoE 等）。

在虚拟模板接口下指定捆绑方式时，可以使用用户名、终端标识符或者两者同时使用。用户名是指 PPP 链路进行 PAP 或 CHAP 认证时所接收到的对端用户名；终端标识符是用来唯一标识一台设备的标志，是指进行 LCP 协商时所接收到的对端终端标识符。系统可以根据接口接收到的用户名或

终端标识符来进行 MP 捆绑，以此来区分虚拟模板接口下的多个 MP 捆绑（对应多条 MP 链路）。

通过虚拟模板接口配置 MP 的具体步骤如表 4-13 所示。

表 4-13　通过虚拟模板接口配置 MP 的步骤

步骤	命令	说明	
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图	
Step 2	**interface virtual-template** *number* 例如： [Sysname] **interface virtual-template** 1	创建并进入虚拟模板接口	
Step 3	**broadcast-limit link** *number* 例如： [Sysname-Virtual-Template1] **broadcast-limit link** 100	（可选）设置虚拟接口模板支持发送组播或广播报文的最大链路数。默认虚拟接口模板支持发送组播或广播报文的最大链路数为 30	
Step 4	**quit** 例如： [Sysname-Virtual-Template1] **quit**	退回系统视图	
Step 5	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	将物理接口与虚拟模板接口关联（有多少个要绑定的物理接口，就要重复执行多少次）	指定与虚拟模板接口关联的物理接口
	ppp mp virtual-template *number* 例如： [Sysname-Serial2/0] **ppp mp virtual-template** 1		配置接口所要绑定的虚拟模板接口
	参见 4.2.2、4.2.3 或 4.2.4 节介绍的 PPP 认证配置		（可选）PPP 认证对 MP 连接的建立没有影响
Step 6	**ppp mp user** *username* **bind virtual-template** *number* 例如： [Sysname] **ppp mp user** user1 **bind virtual-template** 1	将用户名与虚拟模板接口关联（有多少个要采用 MP 的用户，就要重复执行多少次）	建立虚拟模板接口与 MP 用户的对应关系
	interface *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0		指定与虚拟模板接口关联的物理接口
	ppp mp 例如： [Sysname-Serial2/0] **ppp mp**		配置封装 PPP 的接口工作在 MP 方式
	参见 4.2.2、4.2.3 或 4.2.4 节介绍的 PPP 认证配置		（必选）

【注意】上述配置中的第 5 步和第 6 步只能是二选一，不能同时配置。

1．broadcast-limit link 命令

broadcast-limit link *number* 虚拟接口模板视图命令用来设置虚拟接口模板支持发送组播或广播报文的最大链路数。当虚拟接口模板下的链路数目比较多时，所有链路都发送组播或广播报文会影响系统性能，此时可以使用该命令进行限制，使组播或广播报文只在指定数量的链路上发送。参数 *number* 用来指定虚拟接口模板支持发送组播或广播报文的最大链路数，取值范围为 0～128。0 表示不发送组播或广播报文。

默认虚拟接口模板支持发送组播或广播报文的最大链路数为 30，可用 **undo broadcast-limit link** 命令恢复默认设置。

以下示例是设置虚拟接口模板 1 支持发送组播或广播报文的最大链路数为 100。

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] broadcast-limit link 100
```

2．ppp mp virtual-template 命令

ppp mp virtual-template *number* 接口视图命令用来配置物理接口所要绑定的虚拟模板接口号，将该接口绑定到指定的虚拟模板接口上，使接口工作在 MP 方式。配置该命令的接口进行 MP 绑定时，可以不用配置 PAP 或 CHAP 认证。两个或多个配置了相同虚拟模板接口号的接口直接绑定在

一起。另外，该命令与 **ppp mp** 命令互斥，即同一个接口只能配置这两条命令中的一条。

默认接口没有 MP 绑定，工作在普通 PPP 方式下，可用 **undo ppp mp** 命令取消接口的 MP 绑定，配置该接口工作在普通 PPP 方式。

以下示例是配置封装 PPP 的接口 Serial2/0 工作在 MP 方式下，绑定的虚拟模板接口为 Virtual-Template1。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp mp virtual-template 1
```

3．ppp mp user 命令

ppp mp user *username* **bind virtual-template** *number* 系统视图命令用来配置根据用户名进行 MP 捆绑。在 PPP 建立连接的过程中，当 PPP 认证通过后，如果指定了虚拟模板接口，则将按照虚拟模板接口的参数进行 MP 捆绑，并形成一个新的虚拟接口进行数据传输。在虚拟模板接口上可以配置的工作参数包括：本地 IP 地址、为 PPP 对端分配的 IP 地址（或 IP 地址池）和 PPP 工作参数。命令中的参数说明如下：

- *username*：指定绑定时所用的用户名，为 1～80 个字符的字符串。
- **virtual-template** *number*：指定要绑定的虚拟模板接口。参数 *number* 用来指定要绑定的虚拟模板接口号，取值范围为 0～1023。

可用 **undo ppp mp user** 命令取消已经配置的 MP 捆绑。

以下示例是指定用户名 winda 对应的虚拟模板接口为 1，并配置该虚拟模板接口的 IP 地址是 201.138.10.1/24。

```
<Sysname> system-view
[Sysname] ppp mp user winda bind virtual-template 1
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ip address 201.138.10.1 255.255.255.0
```

4．ppp mp 命令

ppp mp 接口视图命令用来配置封装 PPP 的接口工作在 MP 方式。为了增加带宽，可以将多个 PPP 链路捆绑，形成一个逻辑 MP 接口使用。

默认封装 PPP 的接口工作在普通 PPP 方式下，可用 **undo ppp mp** 命令配置该接口工作在普通 PPP 方式下。

以下示例是配置接口 Serial2/0 工作在 MP 方式下。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp mp
```

4.4.3 通过 MP-group 方式配置 MP

上节我们介绍到，MP 的实现方式有两种：一是通过虚拟模板（VT）接口，另一种是通过 MP-group（MP 组）接口。通过 MP-group 方式配置 MP 的具体步骤如表 4-14 所示。

表 4-14 通过 MP-group 方式配置 MP

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface mp-group** *mp-number* 例如： [Sysname] **interface mp-group** 3	创建 MP-group

续表

步骤	命令	说明
Step 3	**ppp mp max-bind** *max-bind-num* 例如： [Sysname-Mp-group3]**ppp mp max-bind** 12	（可选）配置 MP 最大捆绑链路数。默认最大捆绑链路数为 16
Step 4	**ppp mp min-fragment** *size* 例如： [Sysname-Mp-group3] **ppp mp min-fragment** 500	（可选）设置 MP 出报文进行分片的最小报文长度。默认对 MP 报文进行分片的最小报文长度为 128
Step 5	**quit** 例如： [Sysname-Mp-group3] **quit**	退回系统视图
Step 6	**interface** *interface-type interface-number* 例如： [Sysname] **interface serial** 2/0	进入指定接口的视图
Step 7	**ppp mp mp-group** *mp-number* 例如： [Sysname-Serial2/0] **ppp mp mp-group** 3	将接口加入指定的 MP-group

1．interface mp-group 命令

interface mp-group *mp-number* 系统视图命令用来创建 MP-group 接口，并进入指定的 MP-group 接口视图。如果指定的 MP-group 接口已经创建，则该命令用来直接进入 MP-group 接口视图。参数 *mp-number* 用来指定要创建或者要进入的 MP-group 接口的编号，取值范围为 0～1023。该命令与下面将要介绍的 **ppp mp mp-group** 接口视图命令配合使用，但没有先后顺序之分。可用 **undo interface mp-group** 命令删除指定的 MP-group 接口。

以下示例是创建接口 MP-group3。

```
<Sysname> system-view
[Sysname] interface mp-group 3
[Sysname-Mp-group3]
```

2．ppp mp mp-group 命令

ppp mp mp-group *mp-number* 接口视图命令用来将当前接口加入指定的 MP-group，使接口工作在 MP 方式。注意，加入 MP-group 的接口必须是物理接口，Tunnel 接口等逻辑接口不支持该命令。

可用 **undo ppp mp** 命令配置该接口工作在普通 PPP 方式下。

以下示例是将接口 Serial2/0 加入 1 号 MP-group 中。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp mp mp-group 1
```

3．ppp mp max-bind 命令

ppp mp max-bind *max-bind-num* 虚拟模板接口视图/Dialer 接口视图/MP-group 接口视图命令用来配置 MP 最大捆绑链路数。参数 *max-bind-num* 用来指定可以捆绑的最大链路数，取值范围为 1～128。

默认 MP 最大捆绑链路数的值为 16，可用 **undo ppp mp max-bind** 命令恢复默认情况。一般情况下用户不必配置此参数，直接采用默认的 16 条链路。改变此参数配置可能影响 PPP 的性能。

如果 MP 捆绑链路失败，那么很可能是由于最大捆绑链路数小于实际配置的链路捆绑数，请确保最大捆绑链路数要大于实际的捆绑数。在用户改变 MP 的最大捆绑链路数时，改变不能立即生效，必须对所有已捆绑的物理接口进行 **shutdown**/**undo shutdown** 之后改变才会生效。

以下示例是配置 MP 的最大捆绑链路数为 10。

```
<Sysname> system-view
[Sysname] interface virtual-template 0
[Sysname-Virtual-Template0] ppp mp max-bind 10
```

4．ppp mp min-fragment 命令

ppp mp min-fragment *size* 虚拟模板接口视图/Dialer 接口视图/MP-group 接口视图命令用来配置多链路捆绑中对 MP 报文进行分片的最小报文长度。参数 *size* 用来指定对 MP 出报文进行分片的最小报文长度。小于这个值的 MP 报文不进行分片。取值范围为 128～1500 字节。

默认最小报文长度为 128 字节，可用 **undo ppp mp min-fragment** 命令恢复默认值。

【注意】在用户改变这个配置时，改变不能立即生效，必须对所有已捆绑的物理接口进行 **shutdown/undo shutdown** 之后改变才会生效。

以下示例是配置对 MP 报文进行分片的最小报文长度为 500 字节。

```
<Sysname> system-view
[Sysname] interface virtual-template 0
[Sysname-Virtual-Template0] ppp mp min-fragment 500
```

4.4.4 MP 配置示例

本示例拓扑结构如图 4-6 所示。Router A 的 S2/0 接口有两个通道连接到 Router B 的两个通道上，另外两个通道连接到 Router C 的两个通道上，并采用双向 PAP PPP 认证绑定方式。假定 Router A 上的 4 个通道为 Serial2/0:1、Serial2/0:2、Serial2/0:3 和 Serial2/0:4，Router B 上的两个通道的接口名为 Serial2/0:1 和 Serial2/0:2，Router C 上的两个通道的接口名为 Serial2/0:3 和 Serial2/0:4。

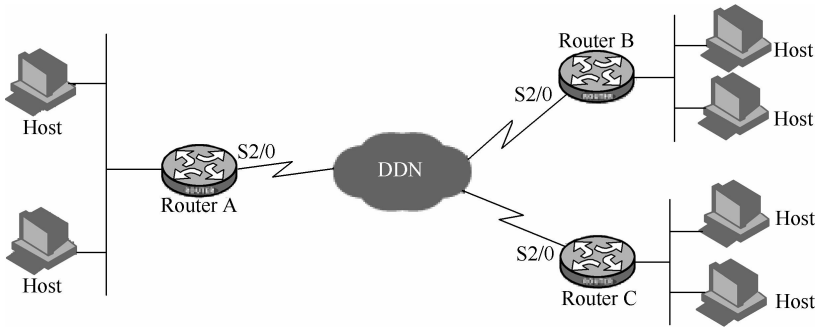

图 4-6　MP 配置示例的拓扑结构

具体配置步骤如下：

（1）Router A 的配置。

1）在 Router A 上为 Router B 和 Router C 各增加一个用户（为了方便介绍现假设用户名和密码分别为 router-b 和 router-c），用于 Router A 认证 Router B 和 Router C。

```
<RouterA> system-view
[RouterA] local-user router-b
[RouterA-luser-router-b] password simple router-b
[RouterA-luser-router-b] service-type ppp
[RouterA-luser-router-b] quit
[RouterA] local-user router-c
[RouterA-luser-router-c] password simple router-c
[RouterA-luser-router-c] service-type ppp
```

2）为这两个用户指定虚拟接口模板。

```
[RouterA-luser-router-c] quit
[RouterA] ppp mp user router-b bind virtual-template 1
[RouterA] ppp mp user router-c bind virtual-template 2
```

3）创建以上所引用的两个虚拟接口模板接口，并配置 IP 地址。

```
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ip address 202.38.166.1 255.255.255.0
[RouterA-Virtual-Template1] quit
[RouterA] interface virtual-template 2
[RouterA-Virtual-Template2] ip address 202.38.168.1 255.255.255.0
[RouterA-Virtual-Template2] quit
```

4）将通道接口（不是子接口）Serial2/0:1、Serial2/0:2、Serial2/0:3 和 Serial2/0:4 加入 MP 通道。在此仅以 Serial2/0:1 为例，其他通道接口作同样的配置。

```
[RouterA] interface serial 2/0:1
[RouterA-Serial2/0:1] link-protocol ppp
[RouterA-Serial2/0:1] ppp mp
[RouterA-Serial2/0:1] ppp authentication-mode pap domain system
[RouterA-Serial2/0:1] ppp pap local-user router-a password simple router-a
[RouterA-Serial2/0:1] quit
```

5）配置域用户使用本地认证方案。

```
[RouterA] domain system
[RouterA-isp-system] authentication ppp local
```

（2）Router B 的配置。

1）为 Router A 增加一个用户。

```
<RouterB> system-view
[RouterB] local-user router-a
[RouterB-luser-router-a] password simple router-a
[RouterB-luser-router-a] service-type ppp
[RouterB-luser-router-a] quit
```

2）为这个用户指定虚拟接口模板，将使用该模板的 NCP 信息进行 PPP 协商。

```
[RouterB] ppp mp user router-a bind virtual-template 1
```

3）配置虚拟接口模板的工作参数。

```
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ip address 202.38.166.2 255.255.255.0
[RouterB-Virtual-Template1] quit
```

4）将接口 Serial2/0:1 和 Serial2/0:2 加入 MP 通道。在此仅以 Serial2/0:1 为例，Serial2/0:2 通道接口作同样的配置。

```
[RouterB] interface serial 2/0:1
[RouterB-Serial2/0:1] ppp mp
[RouterB-Serial2/0:1] ppp authentication-mode pap domain system
[RouterB-Serial2/0:1] ppp pap local-user router-b password simple router-b
```

5）配置域用户使用本地认证方案。

```
[RouterB] domain system
[RouterB-isp-system] authentication ppp local
```

（3）Router C 的配置。

1）为 Router A 增加一个用户。

```
<RouterC> system-view
[RouterC] local-user router-a
[RouterC-luser-router-a] password simple router-a
[RouterC-luser-router-a] service-type ppp
[RouterC-luser-router-a] quit
```

2）为这个用户指定虚拟接口模板，将使用该模板的 NCP 信息进行 PPP 协商。

```
[RouterC] ppp mp user router-a bind virtual-template 1
```

3）配置虚拟接口模板的工作参数。

```
[RouterC] interface virtual-template 1
[RouterC-Virtual-Template1] ip address 202.38.168.2 255.255.255.0
[RouterC-Virtual-Template1] quit
```

4）将通道接口 Serial2/0:3 和 Serial2/0:4 加入 MP 通道。在此仅以 Serial2/0:3 为例，Serial2/0:4

通道接口作同样的配置。

```
[RouterC] interface serial 2/0:3
[RouterC-Serial2/0:1] ppp mp
[RouterC-Serial2/0:1] ppp authentication-mode pap domain system
[RouterC-Serial2/0:1] ppp pap local-user router-c password simple router-c
[RouterC-Serial2/0:1] quit
```

5）配置域用户使用本地认证方案。

```
[RouterC] domain system
[RouterC-isp-system] authentication ppp local
```

4.5 Modem 拨号配置

H3C 路由器的 Modem 拨号是利用其自身所带的 AM（Analog Modem，模拟调制解调器）接口与电话网络的连接进行拨号的。AM 接口就其实现业务而言，类似于“异步串口”和“模拟调制解调器”的组合，对异步串口及 Modem 的绝大部分配置命令都可以在 AM 接口上直接使用。在配置 AM 接口时，可以将 AM 接口看作一种特殊的异步串口。

当然，H3C 路由器也可以外接 Modem 进行拨号访问，这时的配置步骤类似，只是所选择的拨号接口不一样而已，具体的配置步骤如表 4-15 所示。

表 4-15　H3C 路由器 Modem 拨号的配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**dialer-rule** *group-number* { *protocol-name* { **deny** | **permit** } | **acl** { *acl-number* | **name** *acl-name* } } 例如： [Sysname] **dialer-rule** 1 ip **permit**	设定拨号访问组的 DCC（拨号控制中心）呼叫发生的条件
Step 3	**interface Analogmodem** *number*（集成 Modem 时） 或 **interface Serial** *number*（外接 Modem 时） 例如： [Sysname] **interface Analogmodem** 1/0	创建一个 AM 接口，或者指定连接 Modem 的接口
Step 4	**async mode protocol** 例如： [Sysname-Analogmodem1/0]**async mode protocol**	配置异步接口工作在协议模式
Step 5	**ip address** *ip-address mask* 例如： [Sysname-Analogmodem1/0]**ip address** 1.1.1.1 255.255.255.0	为异步接口配置 IP 地址
Step 6	**dialer enable-circular** 例如： [Sysname-Analogmodem1/0] **dialer enable-circular**	启用轮询 DCC 的配置
Step 7	**dialer-group** *group-number* 例如： [Sysname-Serial2/1] **dialer-group** 1	将接口置于一个拨号访问组中
Step 8	**dialer number** *dial-number* 例如： [Sysname-Analogmodem1/0]**dialer number** 6688021	设定去往单个对端的拨号电话号码
Step 9	**user-interface** { *first-num1* [*last-num1*] | { **aux** | **console** | **tty** | **vty** } *first-num2* [*last-num2*] } 例如： [Sysname-Analogmodem1/0]**user-interface tty** 17	进入单一或多个用户界面视图
Step 10	**modem** { **both** | **call-in** | **call-out** } 例如： [Sysname-Analogmodem1/0] **modem call-out**	启用 Modem 的呼入/呼出功能。默认 Modem 的呼入和呼出功能处于禁止状态

下面对其中的主要命令进行说明。

1．dialer-rule 命令

dialer-rule *group-number* { *protocol-name* { **deny** | **permit** } | **acl** { *acl-number* | **name** *acl-name* } }

系统视图命令用来设定拨号访问组的拨号 ACL，从而设定拨号访问组的 DCC（Dial Control Center，拨号控制中心）呼叫发生的条件。可用 **undo dialer-rule** 命令取消该设置。命令中的参数和选项说明如下：

- *group-number*：指定拨号访问组（Dialer Access Group）的序号，取值范围为 1～255，与 **dialer-group** 命令中的 *group-number* 参数相对应。
- *protocol-name*：指定网络协议名，取值为 **ip**（IP 协议）或 **bridge**（网桥协议）。
- **deny**：二选一选项，指定禁止相应协议的报文。
- **permit**：二选一选项，指定允许相应协议的报文。
- *acl-number*：二选一选项，指定拨号访问组所要使用的 ACL 号，取值范围为 2000～3999。
- **name** *acl-name*：二选一选项，指定拨号访问组所要使用的 ACL 名称。通过配置拨号 ACL，可以过滤流经拨号接口的各种报文，根据报文是否符合拨号 ACL 控制列表的通过（permit）或拒绝（deny）条件。

【说明】要想使 DCC 正常发送报文，必须配置正确的 DCC 拨号 ACL，并将对应接口（如物理接口、Dialer 接口）通过 **dialer-group** 命令关联到拨号 ACL，如果缺少此项配置则 DCC 无法正常发送报文。DCC 拨号 ACL 既可以直接配置数据报文的过滤条件，也可以引入 ACL 中的过滤规则。

若一个拨号接口根据配置的 **dialer-group** 找不到对应的 **dialer-rule**，DCC 将报文作为 Uninteresting 报文丢弃。

以下示例是设置 Dialer-rule1 并将它与接口 Serial2/0 关联。

```
<Sysname> system-view
[Sysname] dialer-rule 1 ip permit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer-group 1
```

2．dialer enable-circular 命令

dialer enable-circular 拨号接口（包括物理接口和 Dialer 虚拟接口）视图命令用来启用轮询 DCC（Circular DCC）的配置。

默认接口上不启用任何类型的 DCC，可用 **undo dialer enable-circular** 命令去启用轮询 DCC 的配置。

【说明】DCC 有轮询 DCC（Circular DCC）和共享 DCC（Resoure-Shared DCC）两种配置方式方式。在轮询 DCC 配置方式中，一个逻辑拨号（Dialer）接口可以对应多个物理接口（适用于多用户拨号），而任意一个物理接口只能与一个 Dialer 接口关联，即一个物理接口只能服务于一种拨号服务。每个物理接口既可以借助拨号循环组（Dialer Circular Group）绑定到 Dialer 接口来继承 DCC 参数，又可以直接在物理接口上配置 DCC 参数。服务于同一个拨号循环组的所有物理接口都继承同一个 Dialer 接口的属性，一个 Dialer 接口可以通过配置 **dialer route** 命令对应多个呼叫目的地址，也可以配置 **dialer number** 命令对应单个呼叫目的地址。

而共享 DCC 配置方式中，每个逻辑拨号（Dialer）接口可以对应多个物理接口，同时任意一个物理接口也可服务于多个 Dialer 接口，并且是将物理接口的配置与呼叫的逻辑配置分开进行，再将两者动态地捆绑起来，从而实现同一物理端口为多种不同拨号应用服务。而且，一个 Dialer 接口只对应一个呼叫目的地址，由命令 dialer number 来指定。在物理接口上不能直接配置共享 DCC 参数，物理接口必须通过绑定到 Dialer 接口才能实现共享 DCC 拨号功能。

用户在使用轮询 DCC 前，必须首先使用 **dialer enable-circular** 命令启用轮询 DCC 功能。在取消轮询 DCC 功能后，系统将清除拨号接口下的所有配置信息，而且必须使用 **shutdown/undo shutdown** 命令才能使接口恢复正常。对于非拨号接口，如果非法执行了 **dialer enable-circular** 或 **undo dialer enable-circular** 命令，则必须使用 **shutdown/undo shutdown** 命令使接口恢复正常。

以下示例是在接口 Serial2/0 上启用轮询 DCC。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer enable-circular
```

3．dialer-group 命令

dialer-group *group-number* 拨号接口（物理接口、Dialer 接口）视图命令用来将接口置于一个拨号访问组（Dialer Access Group）中，拨号访问组的拨号规则由 **dialer-rule** 命令指定。

可用 **undo dialer-group** 命令将接口从拨号访问组中删除。

【注意】一个 DCC 接口只能属于一个拨号访问组，重复配置 **dialer-group** 命令则会覆盖上一次的配置。在接口的默认配置中，**dialer-group** 命令是未配置的。用户必须配置此命令，否则 DCC 将无法发送报文。

以下示例是将接口 Serial2/0 置入 Dialer Access Group 1 中。

```
<Sysname> system-view
[Sysname] dialer-rule 1 acl 3101
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer-group 1
```

4．dialer number 命令

dialer number *dial-number* 拨号接口（物理接口、Dialer 接口）视图命令用来设定去往单个对端的拨号号码。参数 *dial-number* 用来指定去往对端的拨号号码，为 1～30 个字符的字符串。当 Dialer 接口或者物理接口作为主叫端时，需要配置此命令。

默认未配置去往对端的拨号串，可用 **undo dialer number** 命令删除已设定的拨号串。

以下示例是设定接口 Dialer1 去往对端的拨号串为 11111。

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer number 11111
```

5．user-interface 命令

user-interface { *first-num1* [*last-num1*] | { **aux** | **console** | **tty** | **vty** } *first-num2* [*last-num2*] }系统视图命令用来进入单一或多个用户界面视图。命令中的参数和选项说明如下：

- *first-num1*：二选一选项，指定第一个用户界面的编号（绝对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准，一般从 0 开始。
- *last-num1*：可选项，指定最后一个用户界面的编号（绝对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准，一般从 0 开始，但不能小于 *first-num1*。
- { **aux** | **console** | **tty** | **vty** }：指定用户界面类型，可多选，具体请参见第 2 章。
- *first-num2*：二选一选项，指定第一个用户界面的编号（相对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准。
- *last-num2*：可选项，指定最后一个用户界面的编号（相对编号方式），不同型号的设备支持的取值范围不同，请以设备的实际情况为准，但不能小于 *first-num2*。

进入单一用户界面视图进行配置后，该配置只对该用户视图有效；进入多个用户界面视图进行配置后，该配置对这些用户视图均有效。

以下示例是进入 Console 用户界面视图。

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0]
```

以下示例是进入 VTY 0～4 用户界面视图。

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4]
```

6．modem 命令

modem { **both** | **call-in** | **call-out** }用户界面视图命令用来配置 Modem 的呼入/呼出权限。命令中的选项说明如下：

- **both**：多选一选项，指定允许 Modem 同时呼入和呼出。
- **call-in**：多选一选项，指定仅允许 Modem 呼入。
- **call-out**：多选一选项，指定仅允许 Modem 呼出。

默认接口上禁止 Modem 呼入和呼出，可用 **undo modem** { **both** | **call-in** | **call-out** }命令取消 Modem 的呼入/呼出权限。

以下示例是配置仅允许 Modem 呼入。

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem call-in
```

4.6　PPPoE ADSL 配置

PPPoE（Point-to-Point Protocol over Ethernet，以太网上的 PPP 协议）可以通过一个远端接入设备为以太网上的主机提供因特网接入服务，并对接入的每个主机实现控制、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 被广泛应用于小区组网等环境中。

PPPoE ADSL 是一种虚拟拨号的 ADSL 接入方式，也是目前最主流的一种 ADSL 接入方式。带 ADSL 接口的 H3C 路由器常用的组网拓扑连接如图 4-7 所示（需要外接 ADSL Modem）。

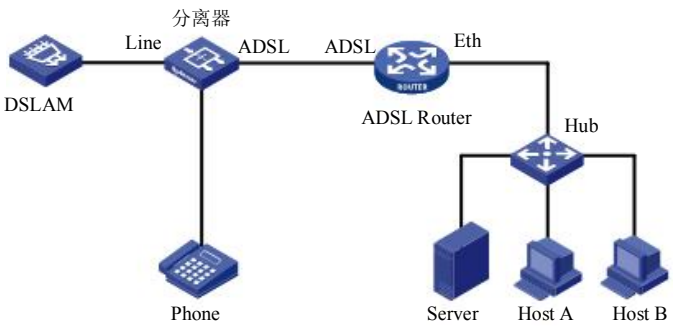

图 4-7　H3C ADSL 路由器的 ADSL 接入拓扑结构

PPPoE 协议采用 Client/Server（客户机/服务器）工作模式，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。H3C 路由器可以配置成 PPPoE 服务器或 PPPoE 客户端两种工作模式。当配置为 PPPoE 服务器时，它支持为 PPPoE 客户端动态分配 IP 地址，提供本地认证、RADIUS/TACACS+等多种认证方式，配合包过滤防火墙及状态防火墙可以对内部网络提供安全保障，适用于校园、智能小区等通过以太网接入 Internet 的组网应用。这种组网方式需要在用户 Host 上安装 PPPoE 客户端拨号软件。

PPPoE 客户端工作模式在 ADSL 宽带接入中被广泛使用。当把路由器配置成 PPPoE 客户端时

（我们通常所使用的宽带路由器都是担当 PPPoE 客户端角色），用户可以不用在 Host 上安装 PPPoE 客户端软件即可接入 Internet，而且同一个局域网中的所有 Host 可以共享一个 ADSL 账号。

4.6.1 配置 PPPoE 服务器

本节先介绍 PPPoE 服务器工作模式的 H3C 路由器配置步骤。PPPoE 服务器可以在物理以太网接口上配置（当使用路由器上集成的 ADSL Modem 时），也可以在由 ADSL 接口生成的虚拟以太网接口上配置（当使用外接的 ADSL Modem 时）。在此仅以在以太网接口上配置为例进行介绍，把 H3C 路由器配置成 PPPoE 服务器的具体配置步骤如表 4-16 所示。

表 4-16 PPPoE 服务器的具体配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface virtual-template** *number* 例如： [Sysname] **interface virtual-template** 1	创建虚拟接口模板并进入虚拟接口模板视图
Step 3	参见 4.2.2、4.2.3、4.2.4 和 4.3 节	（可选）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 IP 地址池）
Step 4	**interface** *interface-type interface-number* 例如： [Sysname] interface ethernet 1/1	进入指定的以太网接口视图
Step 5	**pppoe-server bind virtual-template** *number* 例如： [Sysname-Ethernet1/1] **pppoe-server bind virtual-template** 1	在以太网接口上启用 PPPoE 协议。默认禁止 PPPoE 协议
Step 6	**quit** 例如： Sysname-Ethernet1/1] **quit**	退回系统视图
Step 7	**pppoe-server max-sessions remote-mac** *number* 例如： [Sysname] **pppoe-server max-sessions remote-mac** 50	（可选）配置一个对端 MAC 地址上能创建的最大 PPPoE Session 数目。默认 *number* 数值为 100
Step 8	**pppoe-server max-sessions local-mac** *number* 例如： [Sysname] **pppoe-server max-sessions local-mac** 50	（可选）配置一个本端 MAC 地址上能创建的最大 PPPoE Session 数目。默认 *number* 数值为 100
Step 9	**pppoe-server max-sessions total** *number* 例如： [Sysname] **pppoe-server max-sessions total** 3000	（可选）配置本系统能创建的最大 PPPoE Session 数目（集中式设备）。H3C MSR 系列各型号路由器均为集中式设备。默认系统能创建 PPPoE 会话的最大数目与设备相关，请以设备的实际情况为准
Step 10	**pppoe-server max-sessions slot** *slot-number* **total** *number* 例如： [Sysname] **pppoe-server max-sessions slot** 3 **total** 1500	（可选）配置本系统能创建的最大 PPPoE Session 数目（分布式设备）。不同 I/O 板的默认值不同，请以设备的实际情况为准
Step 11	**pppoe-server max-sessions chassis** *chassis-number* **slot** *slot-number* **total** *number* 例如： [Sysname] **pppoe-server max-sessions chassis** 2 **slot** 3 **total** 1500	（可选）配置本系统能创建的最大 PPPoE Session 数目（分布式 IRF 设备）。不同成员设备上各 I/O 板的默认值不同，请以设备的实际情况为准
Step 12	**pppoe-server log-information off** 例如： [Sysname] **pppoe-server log-information off**	（可选）关闭 PPPoE Server 产生的 PPP 日志信息的显示开关。默认打开 PPPoE Server 产生的 PPP 日志信息的显示开关

1．pppoe-server bind virtual-template 命令

pppoe-server bind virtual-template *number* 系统视图命令用来在连接 ADSL 的以太网接口上启用 PPPoE 协议，将该以太网接口与指定的虚拟模板接口绑定。参数 *number* 用来指定虚拟模板接口

号，取值范围为 0～1023。

默认禁止 PPPoE 协议，可用 **undo pppoe-server bind** 命令在相应接口禁止 PPPoE 协议。

以下示例是在接口 Ethernet1/1 上启用 PPPoE，将接口 Ethernet1/0 与虚拟模板接口 Virtual-Template1 绑定。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] pppoe-server bind virtual-template 1
```

2．pppoe-server max-sessions remote-mac 命令

pppoe-server max-sessions remote-mac *number* 系统视图命令用来配置在一个对端 MAC 地址上能创建 PPPoE 会话的最大数目。参数 *number* 对于集中式设备表示整个系统在一个对端 MAC 地址上能创建 PPPoE 会话的最大数目；对于分布式设备表示每个 I/O 板在一个对端 MAC 地址上能创建 PPPoE 会话的最大数目，取值范围为 1～4096。

默认在一个对端 MAC 地址上能创建 PPPoE 会话的最大数目为 100，可用 **undo pppoe-server max-sessions remote-mac** 命令恢复默认情况。

以下示例是配置在一个对端 MAC 地址上能创建 PPPoE 会话的最大数目为 50。

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions remote-mac 50
```

3．pppoe-server max-sessions local-mac 命令

pppoe-server max-sessions local-mac *number* 系统视图命令用来配置在一个本端 MAC 地址上能创建的 PPPoE 会话的最大数目，也就是一个用户可以打开的最大进程数。参数 *number* 对于集中式设备表示整个系统在一个本端 MAC 地址上能创建 PPPoE 会话的最大数目；对于分布式设备表示每个 I/O 板在一个本端 MAC 地址上能创建 PPPoE 会话的最大数目，取值范围为 1～4096。

默认在一个本端 MAC 地址上能创建的 PPPoE 会话的最大数目为 100，可用 **undo pppoe-server max-sessions local-mac** 命令恢复默认情况。

以下示例是配置在一个本端 MAC 地址上能创建 PPPoE 会话的最大数目为 50。

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions local-mac 50
```

4．pppoe-server max-sessions total 命令

pppoe-server max-sessions total 系统视图命令用来配置系统能创建 PPPoE 会话的最大数目。对于集中式设备，它的完整命令格式为：**pppoe-server max-sessions total** *number*。默认系统能创建 PPPoE 会话的最大数目与设备相关，请以设备的实际情况为准，可用 **undo pppoe-server max-sessions total** 命令恢复默认情况。

对于分布式设备，它的完整命令格式为：**pppoe-server max-sessions slot** *slot-number* **total** *number*。默认系统能创建 PPPoE 会话的最大数目与设备相关，请以设备的实际情况为准，可用 **undo pppoe-server max-sessions slot** *slot-number* 命令恢复默认情况。

对于分布式 IRF（智能弹性架构）设备，它的完整命令格式为：**pppoe-server max-sessions chassis** *chassis-number* **slot** *slot-number* **total** *number*。默认系统能创建 PPPoE 会话的最大数目与设备相关，请以设备的实际情况为准，可用 **undo pppoe-server max-sessions chassis** *chassis-number* **slot** *slot-number* 命令恢复默认情况。

以上命令的可选项和参数说明如下：

- **chassis** *chassis-number*：指定设备在 IRF 中的成员编号，可使用 **display irf** 命令查看。
- **slot** *slot-number*：指定单板的槽位号，取值范围请以设备的实际情况为准。
- *number*：指定系统能创建 PPPoE 会话的最大数目。不同型号的设备支持的取值范围不

同，请以设备的实际情况为准。

以下示例是配置一集中式设备系统能创建 PPPoE 会话的最大数目为 3000。

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions total 3000
```

以下示例是配置一分布式设备 3 号单板能创建 PPPoE 会话的最大数目为 1500。

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions slot 3 total 1500
```

以下示例是配置一分布式 IRF 设备 2 号成员设备的 3 号单板能创建 PPPoE 会话的最大数目为 1500。

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions chassis 2 slot 3 total 1500
```

5．pppoe-server log-information off 命令

pppoe-server log-information off 系统视图命令用来关闭 PPPoE 服务器产生的 PPP 日志信息的显示开关。当终端显示的日志信息太多时，一方面会影响设备的性能，另一方面也会给用户进行配置带来不便。因此，可以在 PPPoE 服务器端关闭日志信息的显示开关。

默认 PPPoE 服务器产生的 PPP 日志信息的显示开关是打开的，即系统显示 PPPoE 服务器产生的 PPP 日志信息，可用 **undo pppoe-server log-information off** 命令打开 PPPoE 服务器产生的 PPP 日志信息的显示开关。

以下示例是关闭 PPPoE 服务器产生的 PPP 日志信息的显示开关。

```
<Sysname> system-view
[Sysname] pppoe-server log-information off
```

4.6.2 配置 PPPoE 客户端的拨号接口

在互联网连接中，用户的 H3C 路由器一般都是用来进行 ADSL 拨号的，所以是作为 PPPoE 客户端的。PPPoE 客户端的配置包括配置拨号接口和配置 PPPoE 会话。

在配置 PPPoE 会话之前，需要先配置一个 Dialer 接口，并在接口上配置 Dialer bundle（拨号捆绑）。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。本节先介绍拨号接口的配置，PPPoE 会话的配置将在下节具体介绍。具体配置步骤如表 4-17 所示。根据需要，可能还要在 Dialer 接口上配置 PPP 认证等相关参数，本节不作介绍，请参见 4.2.2～4.2.4 节。

表 4-17　PPPoE ADSL 拨号接口配置步骤

步骤	命令	说明
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**dialer-rule** *dialer-group* { *protocol-name* { **permit** | **deny** } | **acl** *acl-number* } 例如： [Sysname] **dialer-rule** 1 **acl** 3101	配置 Dialer 规则
Step 3	**interface dialer** *number* 例如： [Sysname] **interface dialer** 1	创建一个拨号接口
Step 4	**dialer user** *username* 例如： [Sysname-Dialer1] **dialer user** routerb	新建一个拨号用户
Step 5	**ip address** { *address mask* | **ppp-negotiate** } 例如： [Sysname- Dialer1] **ip address ppp-negotiate**	配置接口 IP 地址

续表

步骤	命令	说明
Step 6	**dialer bundle** *bundle-number* 例如： [Sysname-Dialer1] **dialer bundle** 3	配置接口的拨号捆绑
Step 7	**dialer-group** *group-number* 例如： [Sysname- Dialer1] **dialer-group** 1	配置接口的拨号组

1．interface dialer 命令

interface dialer *number* 系统视图命令用来创建一个拨号接口。在轮询 DCC 配置中，相当于创建一个拨号轮询组。如果当前已经配置该接口，此命令用来进入该接口视图。参数 *number* 用来指定 Dialer 接口序号，取值范围为 0～1023。

默认没有创建拨号接口，可用 **undo interface dialer** 命令删除一个指定的拨号接口。

Dialer 接口的波特率恒定为 64000bps，并且不能修改为其他值。

以下示例是创建一个接口 Dialer1。

```
<Sysname> system-view
[Sysname] interface dialer 1
```

2．dialer user 命令

dialer user *username* 拨号接口视图命令用来设置拨号用户名，以便接收呼叫时能认证呼叫请求。参数 *username* 是 PPPoE 服务器端创建的本地用户名，为长度 1～80 个字符的字符串。

当拨号接口封装 PPP 时，利用 PPP 认证得到的对端用户名决定接收呼叫时的拨号接口。该命令仅在共享拨号接口上有效。在一个拨号接口下最多可以配置 255 个拨号用户。当一个拨号接口下配置多个 **dialer user** 命令时，就实现了用一个拨号接口同时接入多个用户的连接。

dialer user 命令完成启用共享 DCC 的功能，在已经启用了轮询 DCC 的 Dialer 接口上配置 **dialer user** 命令，则原有的轮询 DCC 相关的拨号配置全部消失。

默认无对端用户名，可使用 **undo dialer user** 命令清除拨号接口下的所有配置信息。

以下示例是设置对端用户名为 lycb。

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer user lycb
```

3．ip address ppp-negotiate 命令

ip address ppp-negotiate 接口视图命令用来为本端接口配置 IP 地址可协商属性，使本端接口接受 PPPoE 分配的 IP 地址。

默认本端接口没有配置 IP 地址可协商属性，可用 **undo ip address ppp-negotiate** 命令取消为本端接口配置 IP 地址可协商属性。

以下示例是为接口 Serial2/0 配置 IP 地址可协商属性。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ip address ppp-negotiate
```

4．dialer bundle 命令

dialer bundle *number* 拨号接口视图命令用来设置工作在共享 DCC 方式的拨号接口使用的 Dialer bundle（拨号捆绑）。参数 *number* 用来指定 Dialer bundle 序号，取值范围为 1～255。此命令仅用于拨号接口，并且一个拨号接口只能使用一个 Dialer bundle。

默认工作在共享 DCC 方式的 Dialer 接口没有指定其使用的 Dialer bundle，可用 **undo dialer**

bundle 命令删除 Dialer 接口使用的 Dialer bundle。

以下示例是在接口 Dialer1 上配置该接口使用 Dialer bundle3。

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer bundle 3
```

5．dialer-group 命令

dialer-group *group-number* 拨号接口（物理接口、Dialer 接口）视图命令用来将接口置于一个拨号访问组（Dialer Access Group）中。用户必须配置此命令，否则 DCC 将无法发送报文。参数 *group-number* 用来指定接口所属的拨号访问组的序号，这个拨号访问组由 **dialer-rule** 命令设定，取值范围为 1～255。一个 DCC 接口只能属于一个 Dialer Access Group，重复配置 dialer-group 命令则会覆盖上一次的配置。

默认情况下，没有配置拨号访问组，可用 **undo dialer-group** 命令将接口从拨号访问组中删除。

以下示例是将接口 Serial2/0 置入 Dialer Access Group 1。

```
<Sysname> system-view
[Sysname] dialer-rule 1 acl 3101
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer-group 1
```

4.6.3 配置 PPPoE 会话

PPPoE 会话有三种工作方式：永久在线方式、报文触发方式、诊断方式。

- 永久在线方式：是指在物理线路 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。
- 报文触发方式：是指在物理线路 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的配置，设备会自动终止 PPPoE 会话。
- 诊断方式：是指路由器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 会话可以在物理以太网接口上配置，也可以在由 ADSL 接口生成的虚拟以太网接口上配置。当设备通过 ADSL 接口连入 Internet 的时候（也就是使用路由器上集成的 ADSL Modem），需要在虚拟以太网接口上配置 PPPoE 会话；当设备通过以太网接口连接 ADSL Modem 再连入 Internet 的时候，需要在以太网接口上配置 PPPoE 会话。

这里仅以在以太网接口上配置为例介绍作为 PPPoE 客户端的 H3C 路由器的 PPPoE 会话配置步骤，如表 4-18 所示。

表 4-18　PPPoE 客户端 PPPoE 会话的配置步骤

步骤	命令	操作
Step 1	**system-view** 例如： <Sysname> **system-view**	进入系统视图
Step 2	**interface ethernet** *interface-number* 例如： [Sysname] **interface** ethernet 1/1	进入以太网接口视图
Step 3	**pppoe-client dial-bundle-number** *number* [**no-hostuniq**] [**diagnose** [**interval** *seconds*] | **idle-timeout** *seconds* [**queue-length** *packets*]] 例如： [Sysname-Ethernet1/1] pppoe-client dial-bundle-number 1	建立一个 PPPoE 会话，并且指定该会话所对应的 Dialer Bundle

以上配置步骤中的 **pppoe-client dial-bundle-number** *number* [**no-hostuniq**] [**diagnose** [**interval** *seconds*] | **idle-timeout** *seconds* [**queue-length** *packets*]]以太网接口视图/虚拟以太网接口视图命令用来建立一个 PPPoE 会话，并且指定该会话所对应的 Dialer Bundle。命令中的参数和选项说明如下：

- **dial-bundle-number** *number*：指定与 PPPoE 会话相对应的 Dialer bundle 编号，取值范围为 1～255。它可用来唯一标识一个 PPPoE 会话，也可以把它作为 PPPoE 会话的编号。
- **no-hostuniq**：可选项，指定在 PPPoE Client 发起的呼叫中不携带 Host-Uniq 字段。默认没有配置 **no-hostuniq** 参数。
- **diagnose**：二选一可选项，指定 PPPoE 会话工作在诊断方式。本参数的支持情况与设备的型号有关，请以设备的实际情况为准。
- **interval** *seconds*：可选项，设置 PPPoE 诊断会话重建时间间隔，取值范围为 5～65535 秒，默认值为 120 秒。本参数的支持情况与设备的型号有关，请以设备的实际情况为准。
- **idle-timeout** *seconds*：二选一可选项，指定允许 PPPoE 会话空闲的时间，取值范围为 1～65535 秒。如果配置本参数，则 PPPoE 会话工作在报文触发方式；如果不配置本参数以及 **diagnose** 参数，则 PPPoE 会话工作在永久在线方式。
- **queue-length** *packets*：可选项，指定在 PPPoE 会话没有建立之前系统可以缓存的报文个数，取值范围为 1～100，默认值为 10。此参数只有在配置了 **idle-timeout** 后才有效。

在一个以太网接口上可以配置多个 PPPoE 会话，即一个以太网接口可以同时属于多个 Dialer Bundle，但是一个 Dialer Bundle 中只能拥有一个以太网接口。PPPoE 会话是和 Dialer Bundle 一一对应的。如果某一拨号接口的 Dialer Bundle 已经有一个以太网接口被用于 PPPoE，那么此 Dialer Bundle 中不能加入其他任何接口。同样，如果在 Dialer Bundle 中已经有除 PPPoE 以太网接口以外的接口，那么此 Dialer Bundle 也同样不能加入被用于 PPPoE Client 的以太网接口。

默认没有配置 PPPoE 会话，可用 **undo pppoe-client** 命令删除一个 PPPoE 会话。无论 PPPoE 会话工作在何种方式，使用 **undo pppoe-client** 命令都会永久删除 PPPoE 会话。如果需要重新建立 PPPoE 会话，用户需要重新配置。**reset pppoe-client** 命令与 **undo pppoe-client** 命令的不同点在于：**reset pppoe-client** 命令仅仅是临时终止 PPPoE 会话，而 **undo pppoe-client** 命令则是永久删除 PPPoE 会话。

以下示例是在接口 Ethernet1/1 上创建一个 PPPoE 会话。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] pppoe-client dial-bundle-number 1
```

4.6.4　PPPoE 服务器配置示例

本示例拓扑结构如图 4-8 所示。示例中，Host A 和 Host B 作为 PPPoE 客户端，通过设备 Router 接入到 Internet。Router 设备作为 PPPoE 服务器，配置本地认证，并通过地址池为用户分配 IP 地址。

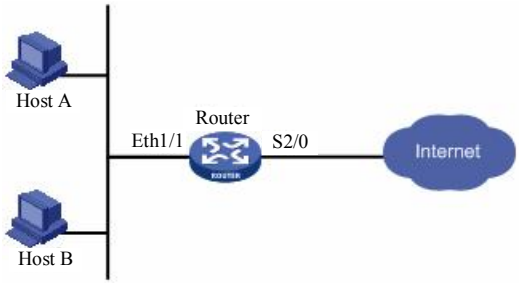

图 4-8　PPPoE 服务器配置示例的拓扑结构

具体的配置步骤如下：

（1）增加一个 PPPoE 客户端用于拨号的 PPPoE 用户 winda。

```
<Sysname> system-view
[Sysname] local-user winda
[Sysname-luser-user1] password simple 123456
[Sysname-luser-user1] service-type ppp
[Sysname-luser-user1] quit
```

（2）创建并配置虚拟模板，指定为 PPPoE 客户端分配 IP 地址的 IP 地址池和本接口 IP 地址。

```
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp authentication-mode chap domain system
[Sysname-Virtual-Template1] ppp chap user winda
[Sysname-Virtual-Template1] remote address pool 1     !---指定为 PPPoE 客户端分配 IP 地址的 IP 地址池
[Sysname-Virtual-Template1] ip address 10.10.1.1 255.0.0.0
[Sysname-Virtual-Template1] quit
```

（3）配置 PPPoE 参数。

```
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] pppoe-server bind virtual-template 1
[Sysname-Ethernet1/1] quit
```

（4）配置域用户使用本地认证方案。

```
[Sysname] domain system
[Sysname-isp-system] authentication ppp local
```

（5）配置用于为 PPPoE 客户端分配 IP 地址的本地 IP 地址池。

```
[Sysname-isp-system] ip pool 1 10.10.1.2 10.10.1.10
```

这样，以太网上各主机安装 PPPoE 客户端软件后，配置好用户名和密码（此处为 winda 和 123456）就能使用 PPPoE 协议，通过设备 Router 接入到 Internet。

若通过 **authentication ppp** 命令配置认证方案为 **radius-scheme** 或 **hwtacacs-scheme**，那么还需要配置 RADIUS/HWTACAS 参数，使系统可以进行认证、授权、计费，具体配置不作介绍。

4.6.5 PPPoE 服务器和客户端配置示例

本示例拓扑结构如图 4-9 所示。示例中，Router A 和 Router B 之间通过各自的 Ethernet1/1 接口相连，要求 Router A 用 PAP/CHAP 方式认证 Router B。其中 Router A 作为 PPPoE 服务器端，Router B 作为 PPPoE 客户端。

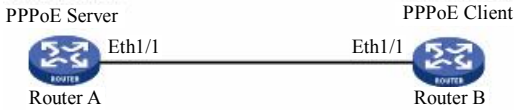

图 4-9　PPPoE 服务器/客户端配置示例的拓扑结构

本示例中的具体配置要区分是采用 PAP 还是 CPAP 认证方式。PAP 认证方式的具体配置如下：

（1）PPPoE 服务器 Router A 的配置。

1）增加用于 PPPoE 客户端拨号的一个 PPPoE 用户 winda。

```
<RouterA> system-view
[RouterA] local-user winda
[RouterA-luser-user2] password simple 123456
[RouterA-luser-user2] service-type ppp
[RouterA-luser-user2] quit
```

2）创建并配置虚拟模板，指定为 PPPoE 客户端 IP 地址和本接口 IP 地址。

```
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ppp authentication-mode pap
[RouterA-Virtual-Template1] ip address 10.10.1.1 255.0.0.0
[RouterA-Virtual-Template1] remote address 10.10.1.2
```

```
[RouterA-Virtual-Template1] quit
```

3）配置 PPPoE 服务器参数。

```
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] pppoe-server bind virtual-template 1
```

（2）PPPoE 客户端 Router B 的配置。

1）配置 PPPoE 客户端参数。

```
<RouterB> system-view
[RouterB] dialer-rule 1 ip permit
[RouterB] interface dialer 1
[RouterB-Dialer1] dialer user winda
[RouterB-Dialer1] dialer-group 1
[RouterB-Dialer1] dialer bundle 1
[RouterB-Dialer1] ip address ppp-negotiate
[RouterB-Dialer1] ppp pap local-user winda password simple 123456
[RouterB-Dialer1] quit
```

2）配置 PPPoE 会话。

```
[RouterB] interface ethernet 1/1
[RouterB-Ethernet1/1] pppoe-client dial-bundle-number 1
```

CHAP 认证方式的具体配置如下：

（1）PPPoE 服务器 Router A 的配置。

1）增加用于 PPPoE 客户端拨号的一个 PPPoE 用户 winda。

```
<RouterA> system-view
[RouterA] local-user winda
[RouterA-luser-user2] password simple 123456
[RouterA-luser-user2] service-type ppp
[RouterA-luser-user2] quit
```

2）创建并配置虚拟模板，指定为 PPPoE 客户端 IP 地址和本接口 IP 地址。

```
[RouterA] interface virtual-template 1
[RouterA-Virtual-Template1] ppp authentication-mode chap
[RouterA-Virtual-Template1] ppp chap user lycb
[RouterA-Virtual-Template1] ip address 10.10.1.1 255.0.0.0
[RouterA-Virtual-Template1] remote address 10.10.1.2
[RouterA-Virtual-Template1] quit
```

3）配置 PPPoE 服务器参数。

```
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] pppoe-server bind virtual-template 1
```

（2）PPPoE 客户端 Router B 的配置。

1）配置 PPPoE 客户端参数。

```
<RouterB> system-view
[RouterB] dialer-rule 1 ip permit
[RouterB] interface dialer 1
[RouterB-Dialer1] dialer user winda
[RouterB-Dialer1] dialer-group 1
[RouterB-Dialer1] dialer bundle 1
[RouterB-Dialer1] ip address ppp-negotiate
[RouterB-Dialer1] ppp chap user winda
[RouterB-Dialer1] quit
[RouterB] local-user lycb
[RouterB-luser-user1] password simple 654321
[RouterB-luser-user1] quit
```

2）配置 PPPoE 会话。

```
[RouterB] interface ethernet 1/1
[RouterB-Ethernet1/1] pppoe-client dial-bundle-number 1
```

4.6.6 利用 ADSL Modem 将局域网接入 Internet 的配置示例

本示例拓扑结构如图 4-10 所示。示例中，局域网内的计算机通过 Router A 访问 Internet，Router A 通过 ADSL Modem 采用永久在线方式接入 DSLAM，Router B 作为 PPPoE 服务器通过 ATM2/0 接口连接至 DSLAM，提供 RADIUS 认证、计费功能（一般位于 ISP 中，所以对于用户来说不用配置）。在 Router A 上启用 PPPoE 客户端功能，局域网内的主机不用安装 PPPoE 客户端软件即可访问 Internet。ADSL 账户的用户名为 user1，密码为 123456。

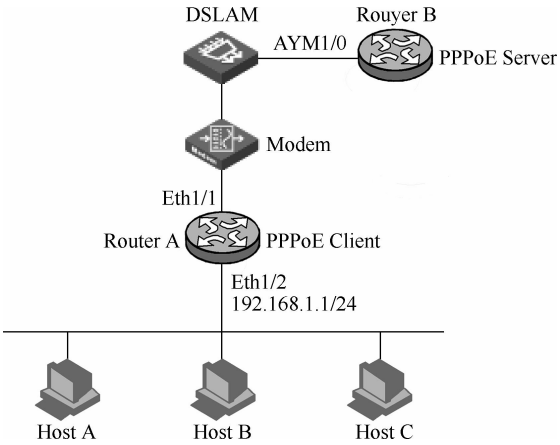

图 4-10 利用 ADSL 将局域网接入 Internet 配置示例的拓扑结构

（1）PPPoE 客户端 Router A 的配置。

1）配置 Dialer 接口。

```
<RouterA> system-view
[RouterA] dialer-rule 1 ip permit
[RouterA] interface dialer 1
[RouterA-Dialer1] dialer-group 1
[RouterA-Dialer1] dialer bundle 1
[RouterA-Dialer1] ip address ppp-negotiate
[RouterA-Dialer1] ppp pap local-user winda password cipher 123456
[RouterA-Dialer1] quit
```

2）配置 PPPoE 会话。

```
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] pppoe-client dial-bundle-number 1
[RouterA-Ethernet1/2] quit
```

3）配置局域网接口及默认路由。

```
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] ip address 192.168.1.1 255.255.255.0
[RouterA-Ethernet1/1] quit
[RouterA] ip route-static 0.0.0.0 0 dialer 1
```

【说明】如果局域网内计算机使用的 IP 地址为私有地址，则还需要在设备上配置 NAT（Network Address Translation，网络地址转换）。NAT 的具体配置方法请参见第 7 章。

（2）PPPoE 服务器 Router B 的配置。

1）增加用于 PPPoE 客户端拨号的一个 PPPoE 用户 winda。

```
<RouterB> system-view
[RouterB] local-user winda
[RouterB-luser-user1] password simple 123456
[RouterB-luser-user1] service-type ppp
[RouterB-luser-user1] quit
```

2）对 ATM 口进行配置。

```
[RouterB] interface atm 1/0
[RouterB-Atm1/0] pvc 0/32
[RouterB-atm-pvc-Atm1/0-0/32] map bridge vrtual-ethernet 1    !---创建 PVC 上到指定虚拟以太网接口上的 IPoEoA 映射或
                                                              !---PPPoEoA 映射
[RouterB-atm-pvc-Atm1/0-0/32] quit
[RouterB-Atm1/0] quit
```

3）在虚拟以太网接口上启用 PPPoE 服务器。

```
[RouterB] interface virtual-ethernet 1
[RouterB-Virtual-Ethernet1] pppoe-server bind virtual-template 1
[RouterB-Virtual-Ethernet1] quit
```

4）在虚拟以太网接口上创建并配置虚拟模板，指定为 PPPoE 客户端分配 IP 地址的 IP 地址池和本接口 IP 地址。

```
[RouterB] interface virtual-template 1
[RouterB-Virtual-Template1] ppp authentication-mode pap domain system
[RouterB-Virtual-Template1] remote address pool 1
[RouterB-Virtual-Template1] ip address 10.10.1.1 255.0.0.0
[RouterB-Virtual-Template1] quit
```

5）配置域用户使用 RADIUS 认证方案。有关 RAIDUS 认证配置请参见《H3C 交换机配置与管理完全手册》（第二版）。通过本示例可以了解在 PPPoE ADSL 接入方式中采用 RADIUS 认证方案的基本配置思路。

```
[RouterB] domain system
[RouterB-isp-system] authentication ppp radius-scheme cams   !---指定 PPP 用户的 RAIDUS 认证方案名为 cams
```

6）创建一个本地 IP 地址池。

```
[RouterB-isp-system] ip pool 1 10.10.1.2 10.10.1.10
[RouterB-isp-system] quit
```

7）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。

```
[RouterB] radius scheme cams !---创建名为 cams 的 RADIUS 认证方式，并进入 RADIUS 认证视图
[RouterB-radius-cams] primary authentication 10.110.91.146 1812   !---指定主 RADIUS 认证服务器
[RouterB-radius-cams] primary accounting 10.110.91.146 1813    !---指定主 RADIUS 计费服务器
[RouterB-radius-cams] key authentication 123456   !---配置 RADIUS 认证的共享密钥
[RouterB-radius-cams] key accounting 654321    !---配置 RADIUS 计费的共享密钥
[RouterB-radius-cams] server-type extended    !--- 指定系统支持的 RADIUS 服务器类型为扩展型
[RouterB-radius-cams] user-name-format with-domain   !---指定发送给 RADIUS 服务器的用户名格式中必须带有 ISP 域
[RouterB-radius-cams] quit
```