H3C SR8800-F 路由器

二层技术-广域网接入配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W101-20210225
产品版本：SR8800FS-CMW710-R8151P25 及以上版本

前 言

本配置指导主要介绍 PPP 等二层广域网链路类型的配置方法。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

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。

1.1.1 PPP 协议

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）。

1.1.2 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。

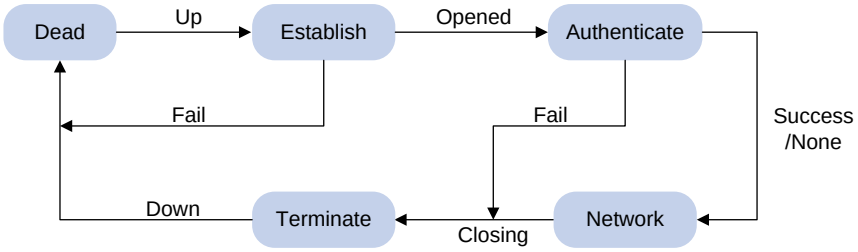
(2) PPP 在 Establish 阶段主要进行 LCP 协商。LCP 协商内容包括：Authentication-Protocol（认证协议类型）、ACCM（Async-Control-Character-Map，异步控制字符映射表）、MRU（Maximum-Receive-Unit，最大接收单元）、Magic-Number（魔术字）、PFC（Protocol-Field-Compression，协议字段压缩）、ACFC（Address-and-Control-Field-Compression，地址控制字段压缩）、MP 等选项。如果 LCP 协商失败，LCP 会上报 Fail 事件，PPP 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 链路还未建立，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



1.1.3 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、认证方未配置用户名。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 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 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。

1.1.4 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，然后在 ISP 域下关联地址池，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。

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。

1.1.5 PPP 支持 IPv6

IPv4 有两种动态地址分配协议，IPCP 协议和 DHPCv4 协议。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。所有认证接入用户都需要使用 ND 协议或 DHCPv6 协议分配 IPv6 全球单播地址和 IPv6 DNS 服务器地址等其它参数。

1. IPv6 地址分配

主机可以通过如下几种方式分配到 IPv6 全球单播地址：

- NDRA 方式：主机通过 ND 协议中的 RA 报文获得 IPv6 地址前缀。主机采用 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 地址前缀的来源按优先级由高到低分为以下几种：

  a. AAA 服务器通过 Framed-IPv6-Prefix 属性授权的 IPv6 前缀。

  b. ISP 域下授权的 IPv6 前缀。

c. ISP 域下授权的 ND 前缀池中的前缀。

d. AAA 服务器通过 Framed-IPv6-Address 属性授权的 128 位 IPv6 全球单播地址中的前缀。（若 AAA 服务器通过 Framed-Interface-Id 属性授权了接口 ID，则忽略本步骤中的前缀，直接跳转到步骤 f）

e. 本地用户视图下通过 **authorization-attribute ipv6** 命令授权的 128 位 IPv6 全球单播地址中的前缀。（若 AAA 服务器通过 Framed-Interface-Id 属性授权了接口 ID，则忽略本步骤中的前缀，直接跳转到步骤 f）

f. 接口下配置的 RA 前缀。

g. 接口下配置的 IPv6 全球单播地址的前缀。

IPv6CP 协商的 IPv6 接口标识按优先级由高到低分为以下几种：

a. AAA 服务器通过 Framed-Interface-Id 属性授权的接口 ID。

b. AAA 服务器通过 Framed-IPv6-Address 属性授权的 128 位 IPv6 全球单播地址中的接口 ID。（若 AAA 服务器通过 Framed-IPv6-Prefix 属性授权了 IPv6 前缀、ISP 域下授权了 IPv6 前缀，或者 ISP 域下授权了 ND 前缀池，则忽略本步骤中的接口 ID，直接跳转到步骤 d）

c. 本地用户视图下通过 **authorization-attribute ipv6** 命令授权的 128 位 IPv6 全球单播地址中的接口 ID。（若 AAA 服务器通过 Framed-IPv6-Prefix 属性授权了 IPv6 前缀、ISP 域下授权了 IPv6 前缀，或者 ISP 域下授权了 ND 前缀池，则忽略本步骤中的接口 ID，直接跳转到步骤 d）

d. ISP 域下配置了 **ipv6cp assign-interface-id** 命令时，由设备自动为 PPP 用户生成的接口 ID。

e. 用户自带的非 0 且和其它接口 ID 不冲突的接口 ID。

f. 用户自带的接口 ID 无效时，由设备自动为 PPP 用户生成的接口 ID。

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”。需要注意的是，AAA 授权 ND 前缀池方式和 IA_NA 方式不能同时配置，二者只配置其中一种。

- DHCPv6（IA_NA）方式：主机通过 DHCPv6 协议申请 IPv6 全球单播地址。在服务器端可以通过 AAA 授权为每个主机分配不同的地址池，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 地址分配给主机。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主机分配地址。关于 DHCPv6 协议的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6”。

  在为用户授权了 IPv6 地址池的情况下，IA_NA 还支持通过以下两种方式为 PPP 用户授权指定的 128 位 IPv6 全球单播地址。

  - AAA 服务器通过 Framed-IPv6-Address 属性授权的 128 位 IPv6 全球单播地址。
  - 本地用户视图下通过 **authorization-attribute ipv6** 命令授权的 128 位 IPv6 全球单播地址。

  需要注意的是，上述两种方式授权的 128 位 IPv6 全球单播地址必须是授权的 IPv6 地址池中的地址，否则不会使用上述两种方式授权的 128 位 IPv6 全球单播地址，而是采用 IPv6 地址池中地址随机分配给用户。

- DHCPv6（IA_PD）方式：Client 端设备通过 DHCPv6 协议申请代理前缀，并使用申请到的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 NDRA 方式或 IA_NA 方式直接为主机分配 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 IA_PD 方式为路由器分配 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。

1.1.6 协议规范

RFC 1661：The Point-to-Point Protocol (PPP)

1.2 PPP配置任务简介

PPP 配置任务如下：

(1) 配置接口封装 PPP 协议

(2) 配置 PPP 认证

请选择以下一项任务进行配置：

- 配置 PAP 认证
- 配置 CHAP 认证（认证方配置了用户名）
- 配置 CHAP 认证（认证方未配置用户名）
- 配置 MSCHAP 或 MSCHAPv2 认证

在网络安全要求较高的环境下，需要配置 PPP 认证。

(3) （可选）配置轮询功能

(4) （可选）配置 PPP 协商参数

- 配置协商超时时间间隔
- 配置 Client 端 PPP 协商 IPv4 地址
- 配置 Server 端 PPP 协商 IPv4 地址
- 配置 Server 端 PPP 协商 IPv6 地址
- 配置接口 IP 网段检查

(5) （可选）配置 PPP 链路质量监测功能

(6) （可选）配置 PPP 协议的魔术字检查功能

1.3 配置接口封装PPP协议

(1) 进入系统视图。

```
system-view
```

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口封装的链路层协议为 PPP。

link-protocol ppp

缺省情况下，除以太网接口、VLAN 接口、ATM 接口外，其它接口封装的链路层协议均为 PPP。

1.4 配置PPP认证

1.4.1 功能简介

PPP 支持的认证方式包括：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。

1.4.2 配置 PAP 认证

1. 配置限制和指导

在认证方上，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。

不论是在本地还是 AAA 服务器上为被认证方配置的用户名和密码必须与被认证方上通过 **ppp pap local-user** 命令配置的用户名和密码相同。

2. 配置认证方

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置本地认证对端的方式为 PAP。

ppp authentication-mode pap [**domain** { *isp-name* | **default enable** *isp-name* }]

缺省情况下，PPP 协议不进行认证。

(4) 配置本地 AAA 认证或者远程 AAA 认证。

具体配置请参见“安全配置指导”中的“AAA”。

3. 配置被认证方

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 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** } *string*

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。

查看配置的密码信息时，无论采用明文或密文加密，密码都将按密文方式显示。

1.4.3 配置 CHAP 认证（认证方配置了用户名）

1. 配置限制和指导

在认证方上，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。

不论是在本地还是 AAA 服务器上为被认证方配置的用户名和密码必须满足如下要求：

- 用户名必须与被认证方上通过 **ppp chap user** 命令配置的被认证方的用户名相同。
- 密码必须与被认证方上为认证方配置的用户名的密码相同。

在被认证方上，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。

不论是在本地还是 AAA 服务器上为认证方配置的用户名和密码必须满足如下要求：

- 用户名必须与认证方上通过 **ppp chap user** 命令配置的认证方的用户名相同。
- 密码必须与认证方上为被认证方配置的用户名的密码相同。

在被认证方上不能通过 **ppp chap password** 命令配置进行 CHAP 认证时采用的密码，否则即使认证方配置了用户名，CHAP 仍将按照认证方未配置用户名的情况进行认证。

2. 配置认证方

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置本地认证对端的方式为 CHAP。

ppp authentication-mode chap [**domain** { *isp-name* | **default enable** *isp-name* }]

缺省情况下，PPP 协议不进行认证。

(4) 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。

(5) 配置本地 AAA 认证或者远程 AAA 认证。

具体配置请参见“安全配置指导”中的“AAA”。

3. 配置被认证方

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 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。

(4) 配置本地 AAA 认证或者远程 AAA 认证。

具体配置请参见“安全配置指导”中的“AAA”。

1.4.4 配置 CHAP 认证（认证方未配置用户名）

1. 配置限制和指导

在认证方上，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。

不论是在本地还是 AAA 服务器上为被认证方配置的用户名和密码必须满足如下要求：

- 用户名必须与被认证方上通过 **ppp chap user** 命令配置的被认证方的用户名相同。
- 密码必须与被认证方上通过 **ppp chap password** 命令配置的密码相同。

2. 配置认证方

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置本地认证对端的方式为 CHAP。

ppp authentication-mode chap [**domain** { *isp-name* | **default enable** *isp-name* }]

缺省情况下，PPP 协议不进行认证。

(4) 配置本地 AAA 认证或者远程 AAA 认证。

具体配置请参见“安全配置指导”中的“AAA”。

3. 配置被认证方

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 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。

(4) 设置 CHAP 认证密码。

ppp chap password { **cipher** | **simple** } *string*

缺省情况下，未配置进行 CHAP 认证时采用的密码。

查看配置的密码信息时，无论采用明文或密文加密，密码都将按密文方式显示。

1.4.5 配置 MSCHAP 或 MSCHAPv2 认证

1. 配置限制和指导

设备只能作为 MSCHAP 和 MSCHAPv2 的认证方来对其它设备进行认证。

MSCHAPv2 认证只有在 RADIUS 认证的方式下，才能支持修改密码机制。

MSCHAPv2 认证时不支持为 PPP 用户配置认证方式为 **none**。

在认证方上，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。不论是在本地还是 AAA 服务器上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相同。

若认证方配置了用户名，则在被认证方上为认证方配置的用户名必须与认证方上 **ppp chap user** 命令配置的用户名相同。

2. 配置认证方（认证方配置了用户名）

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置本地认证对端的方式为 MSCHAP 或 MSCHAPv2。

ppp authentication-mode { **ms-chap** | **ms-chap-v2** } [**domain** { *isp-name* | **default enable** *isp-name* }]

缺省情况下，PPP 协议不进行认证。

(4) 配置采用 MSCHAP 或 MSCHAPv2 认证时认证方的用户名。

ppp chap user *username*

(5) 配置本地 AAA 认证或者远程 AAA 认证。

具体配置请参见“安全配置指导”中的“AAA”。

3. 配置认证方（认证方未配置用户名）

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置本地认证对端的方式为 MSCHAP 或 MSCHAPv2。

ppp authentication-mode { **ms-chap** | **ms-chap-v2** } [**domain** { *isp-name* | **default enable** *isp-name* }]

缺省情况下，PPP 协议不进行认证。

(4) 配置本地 AAA 认证或者远程 AAA 认证。

具体配置请参见“安全配置指导”中的“AAA”。

1.5 配置轮询功能

1. 功能简介

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 周期内没有收到 keepalive 报文的应答，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，则本端不主动发送 keepalive 报文；当本端收到对端主动发送过来的 keepalive 报文时，仍可以对该 keepalive 报文进行应答。

2. 配置限制和指导

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 周期内没有收到 keepalive 报文的应答，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。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口发送 keepalive 报文的周期。

timer-hold *seconds*

缺省情况下，POS 接口和 Serial 接口发送 keepalive 报文的周期为 10 秒。

(4) 配置接口在多少个 keepalive 周期内未收到 keepalive 报文的应答就拆除链路。

timer-hold retry *retry*

缺省情况下，POS 接口和 Serial 接口在 5 个 keepalive 周期内没有收到 keepalive 报文的应答就拆除链路。

1.6 配置PPP协商参数

1.6.1 配置协商超时时间间隔

1. 功能简介

在 PPP 协商过程中，如果协商超时时间间隔内未收到对端的应答报文，则 PPP 将会重发前一次发送的报文。

2. 配置限制和指导

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 协商的延迟时间后，当接口物理层 UP 时 PPP 将在延迟时间超时后才会主

动进行 LCP 协商；如果在延迟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迟时间超时，而是直接进行 LCP 协商。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) （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。

(4) 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。

1.6.2 配置 Client 端 PPP 协商 IPv4 地址

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 为接口配置 IP 地址可协商属性。

ip address ppp-negotiate

缺省情况下，接口未配置 IP 地址可协商属性。

多次执行本命令和 **ip address** 命令，最后一次执行的命令生效。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”。

1.6.3 配置 Server 端 PPP 协商 IPv4 地址

1. 功能简介

目前 Server 端为 Client 端分配 IP 地址支持以下两种方式：

- 从 ISP 域下关联的地址池中为 Client 端分配 IP 地址。
- 从 AAA 服务器直接为 Client 端授权 IP 地址。

2. 配置限制和指导

同时配置以上两种方式时，以 AAA 服务器直接授权的 IP 地址优先，其次是 ISP 域下关联的地址池。

当采用 AAA 服务器直接给 Client 端授权 IP 地址方式时，必须先在 Server 端上通过 **dhcp enable** 命令开启 DHCP 服务，再为 Client 端授权 IP 地址。有关 **dhcp enable** 命令的详细介绍，请参见“三层技术-IP 业务命令参考”中的“DHCP”。

3. 从 ISP 域下关联的 IP 地址池中分配 IP 地址

(1) 进入系统视图。

system-view

(2) 配置 DHCP 功能。

- 如果 Server 端同时作为 DHCP 服务器，则在 Server 端上配置 DHCP 服务器、IP 地址池相关内容。
- 如果 Server 端作为 DHCP 中继，则在 Server 端上配置 DHCP 中继相关内容（必须配置 DHCP 中继用户地址表项记录功能、DHCP 中继地址池），并在远端 DHCP 服务器上配置 IP 地址池。

DHCP 服务器和 DHCP 中继的具体配置介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”和“DHCP 中继”。

(3) 进入 ISP 域视图。

domain name *isp-name*

(4) 在 ISP 域下关联 IP 地址池或 DHCP 中继地址池为 Client 端分配 IP 地址。

authorization-attribute ip-pool *pool-name*

缺省情况下，ISP 域下未关联 IP 地址池或 DHCP 中继地址池。

本命令的详细介绍请参见“安全命令参考”中的“AAA”。

(5) 退回系统视图。

quit

(6) 进入接口视图。

interface *interface-type interface-number*

(7) 配置 Server 端的 IP 地址。

ip address *ip-address*

缺省情况下，接口未配置 IP 地址。

1.6.4 配置 Server 端 PPP 协商 IPv6 地址

1. 通过 NDRA 方式分配 IPv6 地址

(1) 进入接口视图。

interface *interface-type interface-number*

(2) 配置接口自动生成链路本地地址。

ipv6 address auto link-local

(3) 配置 RA 消息中的前缀信息。

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix/prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] * | **no-advertise**]

RA 报文中携带的 IPv6 地址前缀的来源有四种：AAA 授权的 IPv6 前缀、AAA 授权的 ND 前缀池中的前缀、本命令配置的 RA 前缀、接口下配置的 IPv6 全球单播地址的前缀。四种来源的优先级依次降低，AAA 授权的 IPv6 前缀优先级最高。

(4) 关闭对 RA 消息发布的抑制。

undo ipv6 nd ra halt

(5) 配置其他信息配置标志位为 1，即主机通过有状态自动配置（例如 DHCPv6 服务器）获取除 IPv6 地址外的其他信息。

ipv6 nd autoconfig other-flag

(6) 开启 DHCPv6 Server 功能。

ipv6 dhcp select server

(7) 退回至系统视图

quit

(8) 创建 ISP 域并进入其视图。

domain name *isp-name*

(9) 配置当前 ISP 域下的为用户授权 IPv6 前缀。

authorization-attribute ipv6-prefix *ipv6-prefix prefix-length*

2. 通过 IA_NA 方式分配 IPv6 地址

(1) 进入接口视图。

interface *interface-type interface-number*

(2) 配置接口自动生成链路本地地址。

ipv6 address auto link-local

(3) 配置 RA 消息中的前缀信息。

ipv6 nd ra prefix { i*pv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] * | **no-advertise**]

RA 报文中携带的 IPv6 地址前缀的来源有四种：AAA 授权的 IPv6 前缀、AAA 授权的 ND 前缀池中的前缀、本命令配置的 RA 前缀、接口下配置的 IPv6 全球单播地址的前缀。四种来源的优先级依次降低，AAA 授权的 IPv6 前缀优先级最高。

(4) 关闭对 RA 消息发布的抑制。

undo ipv6 nd ra halt

(5) 配置被管理地址的配置标志位为 1，即主机通过有状态自动配置（例如 DHCPv6 服务器）获取 IPv6 地址。

ipv6 nd autoconfig managed-address-flag

(6) 配置其他信息配置标志位为 1，即主机通过有状态自动配置（例如 DHCPv6 服务器）获取除 IPv6 地址外的其他信息。

ipv6 nd autoconfig other-flag

(7) 开启 DHCPv6 Server 功能。

ipv6 dhcp select server

(8) 退回至系统视图。

quit

(9) 配置 IPv6 地址池并在用户认证 ISP 下授权该 IPv6 地址池。

具体配置请参见“三层技术-IP 业务配置指导”中的“DHCPv6”和“AAA”。

3. 通过 IA_PD 方式分配 IPv6 地址

(1) 进入接口视图。

interface *interface-type interface-number*

(2) 配置接口自动生成链路本地地址。

ipv6 address auto link-local

(3) 关闭对 RA 消息发布的抑制。

undo ipv6 nd ra halt

(4) 开启 DHCPv6 Server 功能。

ipv6 dhcp select server

(5) 退回至系统视图

quit

(6) 配置 DHCPv6 前缀地址池并指定包含的前缀和分配的前缀长度。

ipv6 dhcp prefix-pool *prefix-pool-number* **prefix** *prefix/prefix-len* **assign-len** *assign-len*

(7) 创建并进入 IPv6 地址池。

ipv6 pool *pool-name*

(8) 地址池引用前缀池，以便从前缀池中动态选择前缀分配给客户端。

prefix-pool *prefix-pool-number* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

(9) 退回至系统视图

quit

(10) 创建 ISP 域并进入其视图。

domain name *isp-name*

(11) 配置当前 ISP 域下的用户授权属性。

authorization-attribute ipv6-pool *pool-name*

1.6.5 配置接口 IP 网段检查

1. 功能简介

开启接口的 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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启接口的 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。

1.7 配置PPP链路质量监测功能

1. 功能简介

PPP 链路质量监测功能可以实时对 PPP 链路（包括绑定在 MP 中的 PPP 链路）的通信质量（丢包率和错包率）进行监测。

在未配置 PPP 链路质量监测功能之前，PPP 接口（封装 PPP 协议的接口）会每隔一段时间向对端发送 keepalive 报文；在配置此功能之后，PPP 接口会用 LQR（Link Quality Reports，链路质量报告）报文代替 keepalive 报文，即每隔一段时间向对端发送 LQR 报文，用以对链路情况进行监测。

当链路质量正常时，系统对每个 LQR 报文进行链路质量计算，如果连续两次链路质量低于用户设置的禁用链路质量百分比，链路会被禁用。当链路被禁用后，系统每隔十个 LQR 报文进行一次链路质量计算，只有连续三次链路质量高于用户设置的恢复链路质量百分比，链路才会被恢复。因此，当链路被禁用后，至少要在 30 个 keepalive 周期后才能恢复。如果 keepalive 周期设置过大，可能会导致链路长时间无法恢复。

2. 配置限制和指导

当在 PPP 链路两端同时开启链路质量监测功能时，两端设备的参数必须相等。不建议在链路两端同时开启链路质量监测功能。

本特性配置后仅对新接入的用户生效，对当前已经存在用户无影响。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启 PPP 链路质量监测功能。

ppp lqm close-percentage *close-percentage* [**resume-percentage** *resume-percentage*]

缺省情况下，PPP 链路质量监测功能处于关闭状态。

1.8 配置PPP协议的魔术字检查功能

1. 功能简介

在 PPP 链路建立过程中的 LCP 协商阶段会进行 Magic-Number（魔术字）的协商，协商完成后本端和对端均会在本地存储彼此的魔术字。

本端发送 Echo-Request 报文的时候会携带自己的魔术字，在链路两端都开启本功能的情况下，对端收到 Echo-Request 报文后会取出报文中的魔术字与本地存储的对端魔术字进行对比，如果二者相同，则认为链路处于正常状态，并回应携带自己魔术字的 Echo-Reply 报文。本端收到 Echo-Reply 报文后同样取出报文中的魔术字进行检查。

在链路的任何一端，下列任意一种情况发生都将断开链路，并重新进行 LCP 协商。

- 在 keepalive 报文的快速应答功能处于开启状态的情况下：

- 累计收到 5 个 Echo-Request 报文中的魔术字都检查失败。
- 连续收到 5 个 Echo-Reply 报文中的魔术字都检查失败。

- 在 keepalive 报文的快速应答功能处于关闭状态的情况下：
  - 连续收到 5 个 Echo-Request 报文中的魔术字都检查失败。
  - 连续收到 5 个 Echo-Reply 报文中的魔术字都检查失败。

只有开启本功能的一端才会对收到的 Echo-Request 和 Echo-Reply 报文中的魔术字进行检查。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启 PPP 协议的魔术字检查功能。

ppp magic-number-check

缺省情况下，PPP 协议的魔术字检查功能处于关闭状态。

1.9 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 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1-1 PPP 显示和维护

操作	命令
显示PPP的协商报文统计信息	（独立运行模式） **display ppp packet statistics** [**slot** *slot-number*] （IRF模式） **display ppp packet statistics** [**chassis** *chassis-number* **slot** *slot-number*]
清除PPP的协商报文统计信息	（独立运行模式） **reset ppp packet statistics** [**slot** *slot-number*] （IRF模式） **reset ppp packet statistics** [**chassis** *chassis-number* **slot** *slot-number*]

1.10 PPP典型配置举例

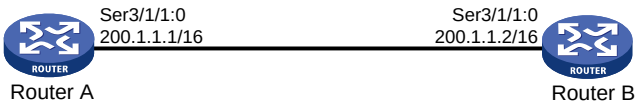
1.10.1 PAP 单向认证配置举例

1. 组网需求

如图 1-2 所示，Router A 和 Router B 之间用接口 Serial3/1/1:0 互连，要求 Router A 用 PAP 方式认证 Router B，Router B 不需要对 Router A 进行认证。

2. 组网图

图1-2 配置 PAP 单向认证组网图



3. 配置步骤

(1) 配置 Router A

为 Router B 创建本地用户。

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

设置本地用户的密码。

```
[RouterA-luser-network-userb] password simple 123456TESTplat&!
```

设置本地用户的服务类型为 PPP。

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

配置接口封装的链路层协议为 PPP（缺省情况下，接口封装的链路层协议为 PPP，此步骤可选）。

```
[RouterA] interface serial 3/1/1:0
[RouterA-Serial3/1/1:0] link-protocol ppp
```

配置本地认证 Router B 的方式为 PAP。

```
[RouterA-Serial3/1/1:0] ppp authentication-mode pap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial3/1/1:0] ip address 200.1.1.1 16
[RouterA-Serial3/1/1:0] quit
```

在系统缺省的 ISP 域 system 下，配置 PPP 用户使用本地认证方案。

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

(2) 配置 Router B

配置接口封装的链路层协议为 PPP（缺省情况下，接口封装的链路层协议为 PPP，此步骤可选）。

```
<RouterB> system-view
[RouterB] interface serial 3/1/1:0
[RouterB-Serial3/1/1:0] link-protocol ppp
```

配置本地被 Router A 以 PAP 方式认证时 Router B 发送的 PAP 用户名和密码。

```
[RouterB-Serial3/1/1:0] ppp pap local-user userb password simple 123456TESTplat&!
```

配置接口的 IP 地址。

```
[RouterB-Serial3/1/1:0] ip address 200.1.1.2 16
[RouterB-Serial3/1/1:0] quit
```

4. 验证配置

通过 **display interface serial** 命令，查看接口 Serial3/1/1:0 的信息，发现接口的物理层和链路层的状态都是 up 状态，并且 PPP 的 LCP 和 IPCP 都是 opened 状态，说明链路的 PPP 协商已经成功，并且 Router A 和 Router B 可以互相 **ping** 通对方。

```
[RouterB] display interface serial 3/1/1:0
Serial3/1/1:0
Current state: UP
Line protocol state: UP
Description: Serial3/1/1:0 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 200.1.1.2/16 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
…略…
[RouterB] ping 200.1.1.1
Ping 200.1.1.1 (200.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 200.1.1.1: icmp_seq=0 ttl=128 time=3.197 ms
56 bytes from 200.1.1.1: icmp_seq=1 ttl=128 time=2.594 ms
56 bytes from 200.1.1.1: icmp_seq=2 ttl=128 time=2.739 ms
56 bytes from 200.1.1.1: icmp_seq=3 ttl=128 time=1.738 ms
56 bytes from 200.1.1.1: icmp_seq=4 ttl=128 time=1.744 ms

--- Ping statistics for 200.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.738/2.402/3.197/0.576 ms
```

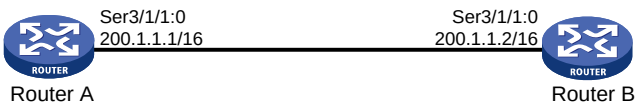
1.10.2 PAP 双向认证配置举例

1. 组网需求

如图 1-3 所示，Router A 和 Router B 之间用接口 Serial3/1/1:0 互连，要求 Router A 和 Router B 用 PAP 方式相互认证对方。

2. 组网图

图1-3 配置 PAP 双向认证组网图



3. 配置步骤

(1) 配置 Router A

为 Router B 创建本地用户。

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

设置本地用户的密码。

```
[RouterA-luser-network-userb] password simple 123456TESTplat&!
```

设置本地用户的服务类型为 PPP。

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

配置接口封装的链路层协议为 PPP（缺省情况下，接口封装的链路层协议为 PPP，此步骤可选）。

```
[RouterA] interface serial 3/1/1:0
[RouterA-Serial3/1/1:0] link-protocol ppp
```

配置本地认证 Router B 的方式为 PAP。

```
[RouterA-Serial3/1/1:0] ppp authentication-mode pap domain system
```

配置本地被 Router B 以 PAP 方式认证时 Router A 发送的 PAP 用户名和密码。

```
[RouterA-Serial3/1/1:0] ppp pap local-user usera password simple 123456TESTplat&!
```

配置接口的 IP 地址。

```
[RouterA-Serial3/1/1:0] ip address 200.1.1.1 16
[RouterA-Serial3/1/1:0] quit
```

在系统缺省的 ISP 域 system 下，配置 PPP 用户使用本地认证方案。

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

(2) 配置 Router B

为 Router A 创建本地用户。

```
<RouterB> system-view
[RouterB] local-user usera class network
```

设置本地用户的密码。

```
[RouterB-luser-network-usera] password simple 123456TESTplat&!
```

设置本地用户的服务类型为 PPP。

```
[RouterB-luser-network-usera] service-type ppp
[RouterB-luser-network-usera] quit
```

配置接口封装的链路层协议为 PPP（缺省情况下，接口封装的链路层协议为 PPP，此步骤可选）。

```
[RouterB] interface serial 3/1/1:0
[RouterB-Serial3/1/1:0] link-protocol ppp
```

配置本地认证 Router A 的方式为 PAP。

```
[RouterB-Serial3/1/1:0] ppp authentication-mode pap domain system
```

配置本地被 Router A 以 PAP 方式认证时 Router B 发送的 PAP 用户名和密码。

```
[RouterB-Serial3/1/1:0] ppp pap local-user userb password simple 123456TESTplat&!
```

配置接口的 IP 地址。

```
[RouterB-Serial3/1/1:0] ip address 200.1.1.2 16
[RouterB-Serial3/1/1:0] quit
```

在系统缺省的 ISP 域 system 下，配置 PPP 用户使用本地认证方案。

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

4. 验证配置

通过 **display interface serial** 命令，查看接口 Serial3/1/1:0 的信息，发现接口的物理层和链路层的状态都是 up 状态，并且 PPP 的 LCP 和 IPCP 都是 opened 状态，说明链路的 PPP 协商已经成功，并且 Router A 和 Router B 可以互相 **ping** 通对方。

```
[RouterB] display interface serial 3/1/1:0
Serial3/1/1:0
Current state: UP
Line protocol state: UP
Description: Serial3/1/1:0 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 200.1.1.2/16 (primary)
Link layer protocol: PPP
LCP opened, IPCP opened
…略…
[RouterB] ping 200.1.1.1
Ping 200.1.1.1 (200.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 200.1.1.1: icmp_seq=0 ttl=128 time=3.197 ms
56 bytes from 200.1.1.1: icmp_seq=1 ttl=128 time=2.594 ms
56 bytes from 200.1.1.1: icmp_seq=2 ttl=128 time=2.739 ms
56 bytes from 200.1.1.1: icmp_seq=3 ttl=128 time=1.738 ms
56 bytes from 200.1.1.1: icmp_seq=4 ttl=128 time=1.744 ms

--- Ping statistics for 200.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.738/2.402/3.197/0.576 ms
```

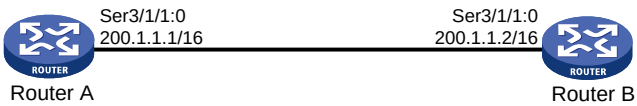
1.10.3 CHAP 单向认证配置举例

1. 组网需求

在图 1-4 中，要求设备 Router A 用 CHAP 方式认证设备 Router B。

2. 组网图

图1-4 配置 CHAP 单向认证组网图



3. 配置方法一（以 CHAP 方式认证对端时，认证方配置了用户名）

(1) 配置 Router A

为 Router B 创建本地用户。

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

设置本地用户的密码。

```
[RouterA-luser-network-userb] password simple 123456TESTplat&!
```

设置本地用户的服务类型为 PPP。

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

配置接口封装的链路层协议为 PPP（缺省情况下，接口封装的链路层协议为 PPP，此步骤可选）。

```
[RouterA] interface serial 3/1/1:0
[RouterA-Serial3/1/1:0] link-protocol ppp
```

配置采用 CHAP 认证时 Router A 的用户名。

```
[RouterA-Serial3/1/1:0] ppp chap user usera
```

配置本地认证 Router B 的方式为 CHAP。

```
[RouterA-Serial3/1/1:0] ppp authentication-mode chap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial3/1/1:0] ip address 200.1.1.1 16
[RouterA-Serial3/1/1:0] quit
```

在系统缺省的 ISP 域 system 下，配置 PPP 用户使用本地认证方案。

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

(2) 配置 Router B

为 Router A 创建本地用户。

```
<RouterB> system-view
[RouterB] local-user usera class network
```

设置本地用户的密码。

```
[RouterB-luser-network-usera] password simple 123456TESTplat&!
```

设置本地用户的服务类型为 PPP。

```
[RouterB-luser-network-usera] service-type ppp
[RouterB-luser-network-usera] quit
```

配置接口封装的链路层协议为 PPP（缺省情况下，接口封装的链路层协议为 PPP，此步骤可选）。

```
[RouterB] interface serial 3/1/1:0
[RouterB-Serial3/1/1:0] link-protocol ppp
```

配置采用 CHAP 认证时 Router B 的用户名。

```
[RouterB-Serial3/1/1:0] ppp chap user userb
```

配置接口的 IP 地址。

```
[RouterB-Serial3/1/1:0] ip address 200.1.1.2 16
[RouterB-Serial3/1/1:0] quit
```

4. 配置方法二（以 CHAP 方式认证对端时，认证方未配置用户名）

(1) 配置 Router A

为 Router B 创建本地用户。

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

设置本地用户的密码。

```
[RouterA-luser-network-userb] password simple 123456TESTplat&!
```

设置本地用户的服务类型为 PPP。

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

配置本地认证 Router B 的方式为 CHAP。

```
[RouterA] interface serial 3/1/1:0
[RouterA-Serial3/1/1:0] ppp authentication-mode chap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial3/1/1:0] ip address 200.1.1.1 16
[RouterA-Serial3/1/1:0] quit
```

在系统缺省的 ISP 域 system 下，配置 PPP 用户使用本地认证方案。

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

(2) 配置 Router B

配置采用 CHAP 认证时 Router B 的用户名。

```
<RouterB> system-view
[RouterB] interface serial 3/1/1:0
[RouterB-Serial3/1/1:0] ppp chap user userb
```

设置缺省的 CHAP 认证密码。

```
[RouterB-Serial3/1/1:0] ppp chap password simple 123456TESTplat&!
```

配置接口的 IP 地址。

```
[RouterB-Serial3/1/1:0] ip address 200.1.1.2 16
[RouterB-Serial3/1/1:0] quit
```

5. 验证配置

通过 **display interface serial** 命令，查看接口 Serial3/1/1:0 的信息，发现接口的物理层和链路层的状态都是 up 状态，并且 PPP 的 LCP 和 IPCP 都是 opened 状态，说明链路的 PPP 协商已经成功，并且 Router A 和 Router B 可以互相 **ping** 通对方。

```
[RouterB] display interface serial 3/1/1:0
Serial3/1/1:0
Current state: UP
Line protocol state: UP
Description: Serial3/1/1:0 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 200.1.1.2/16 (primary)
Link layer protocol: PPP
```

```
LCP opened, IPCP opened
…略…
[RouterB] ping 200.1.1.1
Ping 200.1.1.1 (200.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 200.1.1.1: icmp_seq=0 ttl=128 time=3.197 ms
56 bytes from 200.1.1.1: icmp_seq=1 ttl=128 time=2.594 ms
56 bytes from 200.1.1.1: icmp_seq=2 ttl=128 time=2.739 ms
56 bytes from 200.1.1.1: icmp_seq=3 ttl=128 time=1.738 ms
56 bytes from 200.1.1.1: icmp_seq=4 ttl=128 time=1.744 ms

--- Ping statistics for 200.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.738/2.402/3.197/0.576 ms
```

1.10.4 从 ISP 域下关联的 IP 地址池中分配 IP 地址配置举例

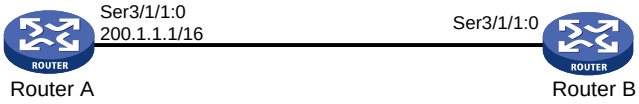
1. 组网需求

Router A 通过 PPP 协商，为 Router B 的接口 Serial3/1/1:0 分配 IP 地址。

要求 Router A 从 ISP 域下关联的 IP 地址池中分配 IP 地址。

2. 组网图

图1-5 从 ISP 域下关联的 IP 地址池中分配 IP 地址组网图



3. 配置步骤

(1) 配置 Router A

开启 DHCP 服务。

```
<RouterA> system-view
[RouterA] dhcp enable
```

创建 IP 地址池 pool1，配置为 DHCP 客户端分配的 IP 地址网段和网关地址。

```
[RouterA] ip pool pool1
[RouterA-ip-pool-pool1] network 200.1.1.0 24
[RouterA-ip-pool-pool1] gateway-list 200.1.1.1
```

将 IP 地址 2.2.2.1 配置为禁用地址。

```
[RouterA-ip-pool-pool1] forbidden-ip 200.1.1.1
[RouterA-ip-pool-pool1] quit
```

为 Router B 创建本地用户。

```
[RouterA] local-user userb class network
```

设置本地用户的密码。

```
[RouterA-luser-network-userb] password simple 123456TESTplat&!
```

设置本地用户的服务类型为 PPP。

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

创建 ISP 域，并在 ISP 域下关联 IP 地址池。

```
[RouterA] domain name dm1
[RouterA-isp-dm1] authorization-attribute ip-pool pool1
[RouterA-isp-dm1] quit
```

配置接口 Serial3/1/1:0 在 ISP 域 dm1 中采用 PAP 方式认证 Router B。

```
[RouterA] interface serial 3/1/1:0
[RouterA-Serial3/1/1:0] ppp authentication-mode pap domain dm1
```

配置接口 Serial3/1/1:0 的 IP 地址。

```
[RouterA-Serial3/1/1:0] ip address 200.1.1.1 16
[RouterA-Serial3/1/1:0] quit
```

(2) 配置 Router B

配置本地被 Router A 以 PAP 方式认证时 Router B 发送的 PAP 用户名和密码。

```
<RouterB> system-view
[RouterB] interface serial 3/1/1:0
[RouterB-Serial3/1/1:0] ppp pap local-user userb password simple 123456TESTplat&!
```

配置接口 Serial3/1/1:0 通过协商获取 IP 地址。

```
[RouterB-Serial3/1/1:0] ip address ppp-negotiate
[RouterB-Serial3/1/1:0] quit
```

4. 验证配置

配置完成后，查看设备 Router B 的接口 Serial3/1/1:0 的概要信息，可见接口 Serial3/1/1:0 通过 PPP 协商获取的 IP 地址为 200.1.1.2。

```
[RouterB] display interface serial 3/1/1:0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Ser3/1/1:0           UP   UP       200.1.1.2
```

在 Router B 上可以 Ping 通 Router A 的 Serial3/1/1:0 接口。

```
[RouterB-Serial3/1/1:0] ping 200.1.1.1
Ping 200.1.1.1 (200.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 200.1.1.1: icmp_seq=0 ttl=128 time=3.197 ms
56 bytes from 200.1.1.1: icmp_seq=1 ttl=128 time=2.594 ms
56 bytes from 200.1.1.1: icmp_seq=2 ttl=128 time=2.739 ms
56 bytes from 200.1.1.1: icmp_seq=3 ttl=128 time=1.738 ms
56 bytes from 200.1.1.1: icmp_seq=4 ttl=128 time=1.744 ms

--- Ping statistics for 200.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.738/2.402/3.197/0.576 ms
```

在 Router A 上可以看到 IP 地址池中已分配一个地址。

```
[RouterA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
200.1.1.2        0030-3030-302e-3030-  Unlimited             Auto(C)
                 3030-2e30-3030-362d
```

2 MP

2.1 MP简介

MP 是 MultiLink PPP 的缩写，是基于增加带宽的考虑，将多个 PPP 通道捆绑成一条逻辑链路使用而产生的。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 通道发送到对端，对端将这些分片组装起来传递给网络层处理。

2.1.1 MP 主要作用

MP 主要是增加带宽的作用，除此之外，MP 还有负载分担的作用，这里的负载分担是链路层的负载分担；负载分担从另外一个角度解释就有了备份的作用。同时，MP 的分片可以起到减小传输时延的作用，特别是在一些低速链路上。

综上所述，MP 的作用主要有以下几个：

- 增加带宽
- 负载分担
- 备份
- 利用分片降低时延

2.1.2 MP 支持的接口类型

MP 能在任何支持 PPP 封装的接口下工作，如串口，建议用户将同一类的接口捆绑使用，不要将不同类的接口捆绑使用。

2.2 MP配置限制和指导

不支持跨业务板进行 MP 捆绑。不支持同一业务板上跨接口卡进行 MP 捆绑，仅支持对同一接口卡内的接口进行 MP 捆绑。

仅 MIC-ET16L、MIC-CLP2L 和 MIC-CLP4L 子卡支持 MP 捆绑。

2.3 MP配置任务简介

MP 配置任务如下：

(1) 通过 MP-group 接口进行 MP 捆绑

(2) （可选）配置 MP 短序协商方式

(3) （可选）配置 MP Endpoint 选项

2.4 配置通过MP-group接口进行MP捆绑

2.4.1 功能简介

MP-group 接口是 MP 的专用接口，不支持其它应用，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。

2.4.2 通过 MP-group 接口进行 MP 捆绑配置任务简介

通过 MP-group 接口配置 MP 配置任务如下：

(1) 创建 MP-group 接口

(2) 将物理接口加入 MP-group 接口

(3) （可选）配置 MP-group 接口的轮询功能

(4) （可选）配置 MP 参数

(5) （可选）恢复当前 MP-group 接口的缺省配置

2.4.3 创建 MP-group 接口

(1) 进入系统视图。

system-view

(2) 创建 MP-group 接口并进入 MP-group 接口视图。

interface mp-group *mp-number*

(3) （可选）配置接口的描述信息。

description *text*

缺省情况下，接口的描述信息为“*该接口的接口名* Interface”，比如：MP-group3/1/1 Interface。

(4) （可选）配置接口的 MTU 值。

mtu *size*

缺省情况下，接口的 MTU 值为 1500 字节。

(5) （可选）配置接口的期望带宽。

bandwidth *bandwidth-value*

缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbps）。

(6) （可选）打开接口。

undo shutdown

缺省情况下，接口处于打开状态。

2.4.4 将物理接口加入 MP-group 接口

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 将接口加入指定的 MP-group 接口，使接口工作在 MP 方式。

ppp mp mp-group *mp-number*

缺省情况下，接口工作在普通 PPP 方式。

2.4.5 配置 MP-group 接口的轮询功能

1. 功能简介

MP-group 接口使用轮询机制来确认链路状态是否正常。

MP-group 接口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。

2. 配置限制和指导

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。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 MP-group 接口视图。

interface mp-group *mp-number*

(3) 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。

(4) 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 *retries*

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。

2.4.6 配置 MP 参数

(1) 进入系统视图。

system-view

(2) 进入 MP-group 接口视图。

interface mp-group *mp-number*

(3) （可选）配置 MP 最大捆绑链路数。

ppp mp max-bind *max-bind-num*

缺省情况下，最大捆绑链路数为 31。

本配置不能立即生效，必须对所有已捆绑的物理接口依次执行 **shutdown** 和 **undo shutdown** 之后改变才会生效。

(4) （可选）配置对 MP 报文进行分片的最小报文长度。

ppp mp min-fragment *size*

缺省情况下，对 MP 报文进行分片的最小报文长度为 128 字节。

(5) （可选）配置 MP 等待期望分片报文的时间。

ppp mp timer lost-fragment *seconds*

缺省情况下，MP 不启动等待期望分片报文的定时器。

(6) （可选）关闭 MP 报文分片功能。

ppp mp fragment disable

缺省情况下，MP 报文分片功能处于开启状态。

(7) （可选）配置 MP 使用严格负载分担模式。

ppp mp load-sharing mode strict-round-robin

缺省情况下，MP 使用智能负载分担模式。

2.4.7 恢复当前 MP-group 接口的缺省配置

1. 配置限制和指导

注意

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 MP-group 接口视图。

interface mp-group *mp-number*

(3) 恢复当前接口的缺省配置。

default

2.5 配置MP短序协商方式

1. 功能简介

MP 捆绑在收发报文时默认使用长序协商方式。其中，长序、短序是指报文序号的长短。

2. 配置限制和指导

配置触发 MP 短序协商仅对配置端接收方向生效，即：

- 如果本端想使用短序方式接收报文，则需要在本端配置触发 MP 短序协商，之后在协商 LCP 的过程本端将添加短序请求，请求对端发送短序，协商通过后，对端使用短序方式发送报文，本端使用短序方式接收报文。
- 如果本端想使用短序方式发送报文，则需要对端配置触发 MP 短序协商，协商通过后，本端使用短序方式发送报文，对端使用短序方式接收报文。

MP 捆绑使用的长短序方式由第一条加入该捆绑中的子通道决定，后续加入捆绑的子通道配置不能更改 MP 捆绑的长短序方式。

如果想使用 MP 短序协商，建议在所有的 MP 子通道下配置触发 MP 短序协商。

配置触发 MP 短序协商会导致当前接口进行 PPP 重协商。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 触发 MP 短序协商，协商成功后本端接收方向将使用短序。

ppp mp short-sequence

缺省情况下，不触发短序协商，使用长序。

2.6 配置MP Endpoint选项

1. 功能简介

在 MP 的 LCP 协商过程会协商 Endpoint 选项（终端描述符）值：在通过 MP-group 接口配置 MP 时，不需要根据 Endpoint 选项值进行 MP 捆绑。当使用 **ppp mp mp-group** 命令将接口加入指定 MP-group 后，接口发送报文中携带的 Endpoint 选项内容缺省为 MP-group 的接口名称，如果用户配置了 Endpoint 选项内容，则携带用户配置的值。

由于 Endpoint 选项内容最长为 20 字节，如果内容超过 20 个字节，则截取前 20 个字节作为 Endpoint 选项内容。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置当前接口在 MP 应用时，LCP 协商的 Endpoint 选项内容。

ppp mp endpoint *endpoint*

缺省情况下，接口发送报文中携带的 Endpoint 选项内容为设备名称。

2.7 MP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 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2-1 MP 显示和维护

操作	命令
显示MP-group接口的相关信息	**display interface** [**mp-group** [*interface-number*]] [**brief** [**description** | **down**]]
显示MP的相关信息	**display ppp mp** [**interface** *interface-type interface-number*]
清除MP-group接口的统计信息	**reset counters interface** [**mp-group** [*interface-number*]]

2.8 MP典型配置举例

2.8.1 通过将链路绑定到 MP-group 接口方式进行 MP 捆绑配置举例

1. 组网需求

设备 Router A 和 Router B 的 Serial3/1/1:0 和 Serial3/1/2:0 分别对应连接。要求通过将链路绑定到 MP-group 接口方式进行 MP 捆绑。

2. 组网图

图2-1 通过将链路绑定到 MP-group 接口方式进行 MP 捆绑组网图

3. 配置步骤

(1) 配置 Router A

创建 MP-group 接口，配置相应的 IP 地址。

```
<RouterA> system-view
[RouterA] interface mp-group 3/1/1
[RouterA-MP-group3/1/1] ip address 1.1.1.1 24
```

配置串口 Serial3/1/1:0。

```
[RouterA-MP-group3/1/1] quit
[RouterA] interface serial 3/1/1:0
[RouterA-Serial3/1/1:0] link-protocol ppp
[RouterA-Serial3/1/1:0] ppp mp mp-group 3/1/1
[RouterA-Serial3/1/1:0] shutdown
[RouterA-Serial3/1/1:0] undo shutdown
[RouterA-Serial3/1/1:0] quit
```

配置串口 Serial3/1/2:0。

```
[RouterA] interface serial 3/1/2:0
[RouterA-Serial3/1/2:0] link-protocol ppp
[RouterA-Serial3/1/2:0] ppp mp mp-group 3/1/1
```

```
[RouterA-Serial3/1/2:0] shutdown
[RouterA-Serial3/1/2:0] undo shutdown
[RouterA-Serial3/1/2:0] quit
```

(2) 配置 Router B

创建 MP-group 接口，配置相应的 IP 地址。

```
[RouterB] interface mp-group 3/1/1
[RouterB-Mp-group3/1/1] ip address 1.1.1.2 24
[RouterB-Mp-group3/1/1] quit
```

配置串口 Serial3/1/1:0。

```
[RouterB] interface serial 3/1/1:0
[RouterB-Serial3/1/1:0] link-protocol ppp
[RouterB-Serial3/1/1:0] ppp mp mp-group 3/1/1
[RouterB-Serial3/1/1:0] shutdown
[RouterB-Serial3/1/1:0] undo shutdown
[RouterB-Serial3/1/1:0] quit
```

配置串口 Serial3/1/2:0。

```
[RouterB] interface serial 3/1/2:0
[RouterB-Serial3/1/2:0] link-protocol ppp
[RouterB-Serial3/1/2:0] ppp mp mp-group 3/1/1
[RouterB-Serial3/1/2:0] shutdown
[RouterB-Serial3/1/2:0] undo shutdown
[RouterB-Serial3/1/2:0] quit
```

4. 验证配置

(1) 在 Router A 上查看绑定效果

查看 MP 的相关信息。

```
[RouterA] display ppp mp
Template: MP-group3/1/1
max-bind: 16, fragment: enabled, min-fragment: 128
Master link: MP-group3/1/1, Active members: 2, Bundle Multilink
Peer's endPoint descriptor: MP-group3/1/1
Sequence format: short (rcv)/long (sent)
Bundle Up Time: 2012/11/04  09:03:16:612
0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved
Sequence: 0 (rcvd)/0 (sent)
Active member channels: 2 members
      Serial3/1/1:0              Up-Time:2012/11/04  09:03:16:613
      Serial3/1/2:0              Up-Time:2012/11/04  09:03:42:945
```

查看 MP-group3/1/1 接口的相关信息。

```
[RouterA] display interface mp-group 3/1/1
MP-group3/1/1
Current state: UP
Line protocol state: UP
Description: MP-group3/1/1 Interface
Bandwidth: 2048kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
```

```
Internet address: 1.1.1.1/24 (primary)
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened
Physical: MP, baudrate: 2048000 bps
Last link flapping: Never
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 2 packets, 80 bytes, 0 drops
Output: 2 packets, 24 bytes, 0 drops
```

在 RouterA 上 ping 对端 IP 地址。

```
[RouterA] ping 1.1.1.2
Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=4.000 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=7.000 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=1.000 ms

--- Ping statistics for 1.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/2.600/7.000/2.577 ms
```

目 录

1 HDLC

1.1 HDLC简介

HDLC（High-level Data Link Control，高级数据链路控制）是一种面向比特的链路层协议，其最大特点是对任何一种比特流（传输的时候是以比特为单位进行传输），均可以实现透明的传输。

1.1.1 HDLC 特点

- HDLC 协议只支持点到点链路，不支持点到多点。
- HDLC 不支持 IP 地址协商，不支持认证。协议内部通过 keepalive 报文来检测链路状态。
- HDLC 协议只能封装在同步链路上。支持 HDLC 协议的接口有：工作在同步模式下的 Serial 接口和 POS 接口。

1.1.2 HDLC 链路状态轮询机制

HDLC 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 HDLC 时，链路层会周期性地向对端发送 keepalive 报文，keepalive 报文中携带了本端发送序号和前一次收到的对端发送序号。当接口发送 keepalive 报文后，如果在 keepalive 周期内收到对端发来的 keepalive 应答报文（该报文携带有本端前一次发送序号），接口下次发送的 keepalive 报文中的发送序号将加一，否则，每经过一个 keepalive 周期，接口将重发一次 keepalive 报文，该报文的发送序号不变。如果 Keepalive 报文重发次数达到上限，在 keepalive 周期内仍然没有收到对端发来的 keepalive 应答报文，链路层会认为对端故障，上报链路层 down。

1.2 配置接口封装HDLC协议

(1) 进入系统视图。

system-view

(2) 进入同步模式的 Serial 接口或 POS 接口视图。

interface *interface-type interface-number*

(3) 在接口封装 HDLC 协议。

link-protocol hdlc

缺省情况下，接口封装 PPP 协议。

1.3 配置轮询功能

1. 配置限制和指导

如果网络的延迟比较大，或拥塞程度较高，可以适当加大 keepalive 报文的发送周期，以避免链路被认为发生故障而被关闭。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 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。

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

建议链路两端的设置保持一致。

(4) 配置允许接口重传的 keepalive 报文个数。

timer-hold retry *retries*

缺省情况下，允许接口重传的 keepalive 报文个数为 5。

1.4 HDLC显示和维护

在完成上述配置后，在任意视图下执行 **display interface** 命令可以查看接口的 HDLC 配置结果。

在用户视图下执行 **reset counters interface** 命令可以清除封装 HDLC 协议接口的统计信息，使接口重新开始统计流量。

表1-1 HDLC 显示和维护

操作	命令
查看接口的HDLC配置结果	**display interface serial** *interface-number* **display interface pos** *interface-number*
清除封装HDLC协议接口的统计信息	**reset counters interface** [**serial** [*interface-number*]] **reset counters interface** [**pos** [*interface-number*]]

1.5 HDLC典型配置举例

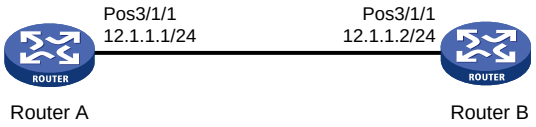
1.5.1 HDLC 基本组网配置举例

1. 组网需求

路由器 Router A 和 Router B 通过 POS 接口相连，要求运行 HDLC 协议。

2. 组网图

图1-1 配置 HDLC 组网图



3. 配置步骤

(1) 配置 Router A

```
<RouterA> system-view
[RouterA] interface pos 3/1/1
[RouterA-Pos3/1/1] clock master
[RouterA-Pos3/1/1] link-protocol hdlc
[RouterA-Pos3/1/1] ip address 12.1.1.1 24
[RouterA-Pos3/1/1] quit
```

(2) 配置 Router B

```
<RouterB> system-view
[RouterB] interface pos 3/1/1
[RouterB-Pos3/1/1] link-protocol hdlc
[RouterB-Pos3/1/1] ip address 12.1.1.2 24
```

4. 验证配置

配置完成后 Router A 和 Router B 可以互相 ping 通。以 Router A 的显示为例。

```
[RouterA] ping 12.1.1.2
Ping 12.1.1.2 (12.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 12.1.1.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 12.1.1.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 12.1.1.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 12.1.1.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 12.1.1.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 12.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

2 HDLC 链路捆绑

2.1 HDLC链路捆绑简介

HDLC 链路捆绑是将多个链路层协议为 HDLC 的接口（简称 HDLC 接口）捆绑到一起，形成一条逻辑上的数据链路。

2.1.1 技术优点

HDLC 链路捆绑的作用如下：

- 流量负载分担：出/入流量可以在多个成员接口之间分担。
- 增加带宽：链路捆绑接口的带宽是各可用成员接口带宽的总和。
- 提高连接可靠性：当某个成员接口出现故障时，流量会自动切换到其他可用的成员接口上，从而提高整个捆绑链路的连接可靠性。

2.1.2 基本概念

1. HDLC 捆绑接口

HDLC 捆绑接口是一个逻辑接口。一个 HDLC 捆绑接口对应一个 HDLC 捆绑。

2. HDLC 捆绑

HDLC 捆绑是一组 HDLC 接口的集合。HDLC 捆绑是随着 HDLC 捆绑接口的创建而自动生成的，其编号与 HDLC 捆绑接口编号相同。

3. 成员接口

加入 HDLC 捆绑后的接口称为成员接口。目前，只有 POS 接口可以加入 HDLC 捆绑，并且加入 HDLC 捆绑的成员接口的链路层协议类型必须是 HDLC。

加入 HDLC 捆绑后，成员接口的网络层将被置于 down 状态，成员接口上的三层业务相关的配置都不生效，成员接口通过 HDLC 捆绑接口的三层配置进行业务处理。

2.1.3 成员接口状态

成员接口有下列 4 种状态：

- 初始状态：成员接口的链路层协议处于 down 状态。
- 协商状态：成员接口的链路层协议处于 up 状态，但是成员接口不满足选中条件。
- 就绪状态：成员接口的链路层协议处于 up 状态，且成员接口满足选中条件，但由于最多选中成员接口数目/最少选中成员接口数目/最小激活带宽的限制，使得该成员接口没有被选中，那么该成员接口将处于就绪状态。
- 选中状态：成员接口的链路层协议处于 up 状态，且成员接口满足选中条件，处于选中状态。只有处于此状态的成员接口才能转发流量。

如果 HDLC 捆绑中没有处于选中状态的成员接口，则 HDLC 捆绑接口将处于 down 状态，不能转发流量；只有 HDLC 捆绑中有处于选中状态的成员接口，HDLC 捆绑接口才会处于 up 状态，才能进行流量转发。HDLC 捆绑的带宽是所有处于选中状态的成员接口的带宽之和。

成员接口状态的确定过程如下：

(1) 当成员接口的链路层协议处于 down 状态时，成员接口将处于初始状态，当成员接口的链路层协议变为 up 状态后，成员接口先是处于协商状态，之后经过下面的选择过程可能变为选中状态或就绪状态。

(2) 假设处于协商状态的成员接口有 M 个、设备限制最多选中成员接口数目为 N[1]，当 M<=N 时，这 M 个成员接口均处于选中状态；当 M>N 时，依次按照成员接口的速率/波特率 > 捆绑优先级 > 接口索引号对这些成员接口进行排序（速率/波特率大的排在前面、捆绑优先级高的排在前面，接口索引号小的排在前面），排在前 N 个的成员接口将处于选中状态，排在后面的（M-N）个成员接口将处于就绪状态。

(3) 假设步骤（2）中选出的处于选中状态的成员接口有 P 个、设备限制的最少选中成员接口数目为 Q，当 P<Q 或者这 P 个成员接口的总带宽小于配置的最小激活带宽时，这 P 个成员接口都不会被选中，将处于就绪状态；当 P>=Q 或者设备没有限制最少选中成员接口数目和最小激活带宽时，这 P 个成员接口将处于选中状态。


说明

[1]: 设备限制的最多选中成员接口数目首先采用用户通过 **bundle max-active links** 命令配置的值；如果用户未配置，则采用设备支持的最多选中成员接口数目 8。

2.2 配置HDLC捆绑接口

2.2.1 配置 HDLC 捆绑接口基本功能

1. 配置限制和指导

- 为保证转发正常，建议在同一条 HDLC 捆绑链路两端的 HDLC 捆绑接口上配置相同的最少选中成员接口数目、最多选中成员接口数目、最小激活带宽。
- HDLC 链路捆绑配置完成后，如果用户修改了最少选中成员接口数目、最多选中成员接口数目、最小激活带宽，那么设备会重新确定各成员接口的状态。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 HDLC 捆绑接口并进入 HDLC 捆绑接口视图。

interface hdlc-bundle *bundle-id*

(3) （可选）配置最小激活带宽。

bundle min-active bandwidth *bandwidth*

缺省情况下，不进行限制。

(4) 配置最少选中成员接口数目。

bundle min-active links *number*

缺省情况下，不进行限制。

配置的最少选中成员接口数目不能大于最多选中成员接口数目。

(5) 配置最多选中成员接口数目。

bundle max-active links *number*

缺省情况下，以设备支持的最多选中成员接口数目为 8。

(6) （可选）配置接口的期望带宽。

bandwidth *bandwidth-value*

缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbit/s）。

接口的期望带宽会影响链路开销值，具体介绍请参见“三层技术-IP 路由配置指导”中的“OSPF”、“OSPFv3”和“IS-IS”。

(7) （可选）配置 HDLC 捆绑接口的描述信息。

description *text*

缺省情况下，接口的描述信息为“*该接口的接口名* Interface”。

(8) （可选）配置 HDLC 捆绑接口的 MTU 值。

mtu *size*

缺省情况下，HDLC 捆绑接口的 MTU 值为 1500 字节。

MTU 参数会影响 IP 报文的分片与重组，可以通过本命令来设置合适的 MTU 值。

(9) 打开 HDLC 捆绑接口。

undo shutdown

缺省情况下，HDLC 捆绑接口处于打开状态。

当打开 HDLC 捆绑接口时，会触发重新确定成员接口的状态；当关闭 HDLC 捆绑接口时，所有选中成员口都会变成协商状态。

2.2.2 恢复 HDLC 捆绑接口的缺省配置

1. 配置限制和指导

说明

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行本配置前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 HDLC 捆绑接口视图。

interface hdlc-bundle *bundle-id*

(3) 恢复 HDLC 捆绑接口的缺省配置。

default

2.3 配置接口加入HDLC捆绑

1. 配置限制和指导

- 只有物理 POS 接口可以加入 HDLC 捆绑。
- 一个接口只能加入一个 HDLC 捆绑，如果需要加入其他 HDLC 捆绑，必须先退出原来的 HDLC 捆绑。
- 加入 HDLC 捆绑的接口封装的链路层协议必须为 HDLC。接口加入 HDLC 捆绑之后不允许修改链路层协议。
- 可以将不同接口板上的接口加入到同一个 HDLC 捆绑。
- HDLC 链路捆绑配置完成后，如果用户修改了某成员接口的捆绑优先级，那么设备会重新确定各成员接口的状态。
- HDLC 捆绑接口没有创建的情况下，也允许将接口加入 HDLC 捆绑。
- 如果本地设备使用了 HDLC 捆绑，与该 HDLC 捆绑的成员接口直连的对端设备上的接口也必须加入同一个 HDLC 捆绑。两端设备上的 HDLC 捆绑编号不要求相同，HDLC 捆绑编号只具有本地意义。
- **bundle member-priority** 命令和 **bundle max-active links** 命令一般需要配合使用，以保证两台设备相互连接的接口能够同时处于选中状态（只有两端接口同时处于选中状态，报文才能发送成功），避免出现一端接口处于选中状态，而另一端接口没有处于选中状态的情况。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 POS 接口视图。

interface *interface-type interface-number*

(3) 配置接口的链路层协议类型为 HDLC。

link-protocol hdlc

缺省情况下，接口的链路层协议为 PPP。

加入 HDLC 捆绑的接口封装的链路层协议必须为 HDLC。

(4) 配置接口加入 HDLC 捆绑。

bundle id *bundle-id*

缺省情况下，接口不属于任何 HDLC 捆绑。

一个接口只能加入一个 HDLC 捆绑，如果需要加入其他 HDLC 捆绑，必须先退出原来的 HDLC 捆绑。

可以将不同接口板上的接口加入到同一个 HDLC 捆绑。

(5) 配置接口的捆绑优先级。

bundle member-priority *priority*

缺省情况下，接口的捆绑优先级为 32768。

HDLC 链路捆绑配置完成后，如果用户修改了某成员接口的捆绑优先级，那么设备会重新确定各成员接口的状态。

2.4 HDLC链路捆绑显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 HDLC 链路捆绑的运行情况，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 HDLC 捆绑接口的统计信息。

表2-1 HDLC 链路捆绑显示和维护

操作	命令
显示HDLC捆绑信息	**display bundle hdlc-bundle** [*bundle-id*]
显示HDLC捆绑接口的相关信息	**display interface** [**hdlc-bundle** [*bundle-id*]] [**brief** [**description** | **down**]]
清除HDLC捆绑接口的统计信息	**reset counters interface** [**hdlc-bundle** [*bundle-id*]]

2.5 HDLC链路捆绑典型配置举例

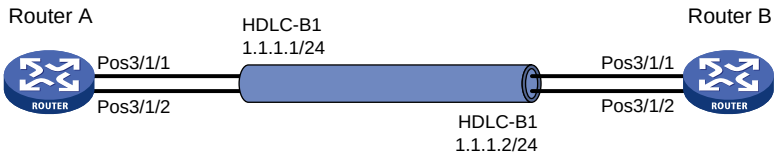
2.5.1 HDLC 链路捆绑基本组网配置举例

1. 组网需求

为了增加 Router A 和 Router B 之间的链路带宽，并提高连接可靠性，在设备之间建立 HDLC 捆绑逻辑链路。

2. 组网图

图2-1 配置 HDLC 链路捆绑组网图



3. 配置步骤

(1) 配置 Router A

创建 HDLC 捆绑接口 1，并配置 IP 地址。

```
<RouterA> system-view
[RouterA] interface hdlc-bundle 1
[RouterA-HDLC-bundle1] ip address 1.1.1.1 24
[RouterA-HDLC-bundle1] quit
```

将 Pos3/1/1、Pos3/1/2 加入到 HDLC 捆绑 1（POS 接口采用主时钟模式）。

```
[RouterA] interface pos 3/1/1
[RouterA-Pos3/1/1] clock master
[RouterA-Pos3/1/1] link-protocol hdlc
[RouterA-Pos3/1/1] bundle id 1
[RouterA-Pos3/1/1] quit
[RouterA] interface pos 3/1/2
[RouterA-Pos3/1/2] clock master
[RouterA-Pos3/1/2] link-protocol hdlc
[RouterA-Pos3/1/2] bundle id 1
[RouterA-Pos3/1/2] quit
```

(2) 配置 Router B

创建 HDLC 捆绑接口 1，并配置 IP 地址。

```
<RouterB> system-view
[RouterB] interface hdlc-bundle 1
[RouterB-HDLC-bundle1] ip address 1.1.1.2 24
[RouterB-HDLC-bundle1] quit
```

将 Pos3/1/1、Pos3/1/2 加入到 HDLC 捆绑 1。

```
[RouterB] interface pos 3/1/1
[RouterB-Pos3/1/1] link-protocol hdlc
[RouterB-Pos3/1/1] bundle id 1
[RouterB-Pos3/1/1] quit
[RouterB] interface pos 3/1/2
[RouterB-Pos3/1/2] link-protocol hdlc
[RouterB-Pos3/1/2] bundle id 1
[RouterB-Pos3/1/2] quit
```

4. 验证配置

Router A 和 Router B 的 HDLC 捆绑接口能够互相 Ping 通。

```
[RouterA] ping –a 1.1.1.1 1.1.1.2
Ping 1.1.1.2 (1.1.1.2) from 1.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 1.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.000/0.000/0.000 ms
```

在 Router A 或 Router B 上执行 **display bundle hdlc-bundle** 命令，可以看到 HDLC 捆绑接口 1 的捆绑信息。以 Router A 的显示为例。

```
[RouterA] display bundle hdlc-bundle 1 slot 3
Bundle: HDLC-bundle1, slot 3
  Selected members: 2, Total bandwidth: 1244160 kbps
  Member              State               Bandwidth(kbps)     Priority
  Pos3/1/1            Selected            622080              32768
  Pos3/1/2            Selected            622080              32768
```

上述信息表明，Pos3/1/1 和 Pos3/1/2 都处于选中状态，可以进行流量的负载分担；HDLC 捆绑的带宽为 1244160 kbps，是两个 POS 接口的带宽之和；当其中一个 POS 接口出现故障时，流量可以通过另一个 POS 接口发送，提高了链路的连接可靠性。

目 录

1 ATM

1.1 ATM简介

ATM（Asynchronous Transfer Mode，异步传输模式）技术是以分组传输模式为基础并融合了电路传输模式高速化的优点发展而成。由于它的灵活性以及对多媒体业务的支持，被认为是实现宽带通信的核心技术。

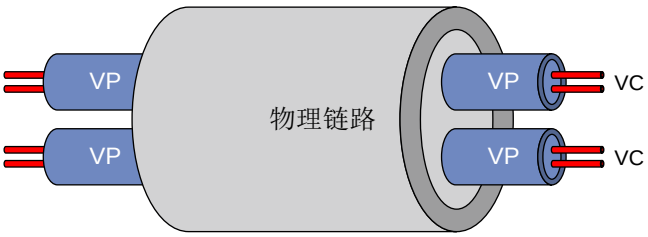
1.1.1 ATM 信元

根据 ITU-T 定义，ATM 是以信元为基本单位进行信息传输、复用和交换的。ATM 信元具有 53 字节的固定长度，其中前 5 个字节是信元头，其余 48 个字节是有效载荷。ATM 信元头的功能有限，主要用来标识虚连接，另外也完成了一些功能有限的流量控制，拥塞控制，差错控制等功能。

1.1.2 ATM 连接和 ATM 交换

ATM 是面向连接的交换，其连接是逻辑连接，即虚连接。ATM 网络中，可以在物理链路上创建逻辑连接 VP（Virtual Path，虚路径）和 VC（Virtual Circuit，虚电路）。如图 1-1 所示，一条物理链路上可以创建多条 VP，每个 VP 可以采用复用方式容纳多个 VC。不同用户的信元通过不同的 VP 和 VC 传递。VP 和 VC 通过 VPI（Virtual Path Identifier，虚路径标识符）和 VCI（Virtual Channel Identifier，虚通道标识符）来标识。ATM 使用一对 VPI/VCI 的组合来标识一条虚连接。

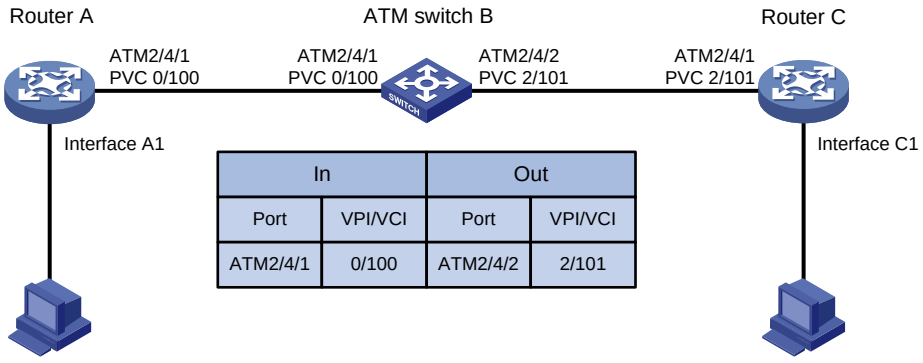
图1-1 VP、VC 和物理链路关系



目前，ATM 接口只支持手工配置的 PVC（Permanent Virtual Circuit，永久虚电路），不支持通过信令建立的 SVC（Switched Virtual Circuit，交换虚电路）。每条 PVC 通过 VPI/VCI 值来标识。

在 ATM 网络中，通过查找 ATM 交换机的交换表项改变 VPI/VCI 值，实现 ATM 信元的转发。在 PVC 方式下，ATM 交换机的交换表项由网管配置，由网管统一分配 VPI/VCI 值，用户根据网管分配的 VPI/VCI 值来配置路由器上的 PVC。如果两台 ATM 设备的 ATM 接口直连，两端 ATM 接口下配置的 VPI/VCI 值必须相同。典型的 ATM 交换过程如图 1-2 所示，从路由器 Router A 的 ATM2/4/1 接口的 PVC 0/100 发送的 ATM 信元，到达 ATM 交换机 ATM switch B 的 ATM2/4/1 接口的 PVC 0/100 后，通过查找交换表项，从 ATM2/4/2 接口的 PVC 2/101 转发出去，最终到达路由器 Router C 的 ATM2/4/1 接口的 PVC 2/101。

图1-2 ATM 交换示意图



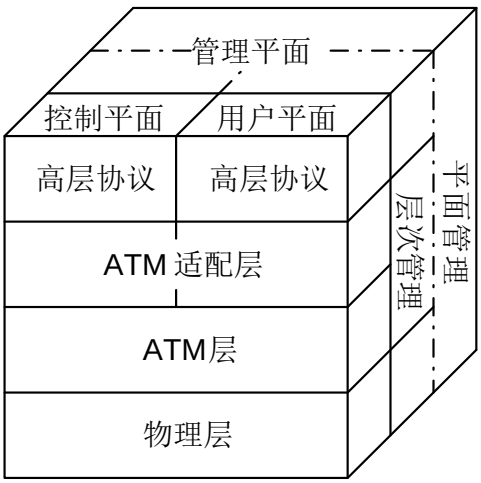
1.1.3 ATM 层次结构

ATM 基本协议框架分为 3 个平面，即用户平面、控制平面和管理平面。用户平面和控制平面又各分为 4 层，即物理层、ATM 层、ATM 适配层和高层，在各层中还有更精细的子层划分。

- 控制平面主要利用信令协议来完成连接的建立和拆除。
- 管理平面又分为层次管理和平面管理。其中层次管理负责各平面中各层的管理，具有与其它平面相对应的层次结构；平面管理负责系统的管理和各平面之间的通信。

各平面与各层的关系如图 1-3。

图1-3 ATM 协议模型图



各层的具体功能如下：

- 物理层主要提供 ATM 信元的传输通道，将 ATM 层传来的信元加上其传输开销后形成连续的比特流；同时，在接收到物理媒介上传来的连续比特流后，取出有效信元传递给 ATM 层。
- ATM 层在物理层之上，利用物理层提供的服务，与对等层进行以信元为单位的通信。ATM 层与物理媒介的类型和物理层的具体实现无关，与具体传送的业务类型也无关。从 ATM 适配层输入 ATM 层的是 48 字节的净荷，这 48 字节的净荷被称为分段和重组协议数据单元（SAR-PDU），而 ATM 层输出的则是 53 字节的信元，该信元将传送到物理层进行传输。ATM

层负责产生 5 个字节的信元头，信元头将加到净荷的前面。ATM 层的其他功能包括虚路径标识符/虚通道标识符（VPI/VCI）传输、信元多路复用/分用以及一般流量控制。

- AAL（ATM Adaptation Layer，ATM 适配层）是高层协议与 ATM 层间的接口，它负责转接 ATM 层与高层协议之间的信息。目前，已经提出 4 种类型的 AAL：AAL1、AAL2、AAL3/4 和 AAL5，每一种类型分别支持 ATM 网络中某些特征业务。H3C 产品采用 AAL5 来支持数据通信业务。
- ATM 高层协议则主要具有 WAN 互连、与现有三层协议互连、承载 IP 协议功能。

1.1.4 ATM 服务类型

ATM 支持四种服务类型：

- CBR（Constant Bit Rate，确定比特率）
- UBR（Unspecified Bit Rate，不确定比特率）
- VBR-RT（Variable Bit Rate-Real Time，实时可变速率）
- VBR-NRT（Variable Bit Rate-Non Real Time，非实时可变速率）

这些服务类型的选择与网络的 QoS 需求有关。

1. CBR

CBR 服务用于在连接的生命期中需要静态带宽的连接。这个带宽由 PCR（Peak Cell Rate，峰值信元速率）值来确定。在 CBR 服务中，源端可以持续地以峰值信元速率发送信元。

CBR 服务一般用来支持对时延变化要求较高的实时业务（例如：语音、视频）。

2. VBR-RT

VBR-RT 服务也是一种实时的应用，对时延和抖动有严格的限制，VBR-RT 的主要应用有语音和视频业务。

VBR-RT 连接的指标主要靠 PCR、SCR（Sustainable Cell Rate，可持续信元速率）、MBS（Maximum Burst Size，最大突发长度）来描述。源端可以在平均信元速率为 SCR 的情况下，以 PCR 的速率发送最大信元个数为 MBS 的突发流量而不丢信元。

3. VBR-NRT

VBR-NRT 服务支持突发性的非实时的应用，该特性是通过 PCR、SCR 以及 MBS 来描述的。对那些满足流量合同的信元，VBR-NRT 服务可以保证很低的信元丢失率但是不保证时延。

4. UBR

UBR 服务用于对时延和带宽都要求不高的应用。UBR 服务不保证服务质量，连接的信元丢失率和信元传输时延均没有数值保证，如果发生拥塞，UBR 服务的信元最先被丢弃。

1.1.5 ATM 应用

ATM 支持 IPoA 应用方式。

IPoA（IP over ATM，在 ATM 上承载 IP 协议）：ATM 为处在同一网络内的 IP 主机之间的通信提供数据链路层，同时将 IP 报文封装在 ATM 信元中。ATM 作为 IP 业务的承载网提供了优良的网络性能和完善、成熟的 QoS 保证。

1.1.6 ATM OAM

OAM 的名词存在两种不同解释，主要是针对不同的协议而言。

- OAM：Operation And Maintenance（ITU-T I.610 02/99）
- OAM：Operation Administration and Maintenance（LUCENT APC User Manual，03/99）

OAM 提供了一种不中断业务的故障检测、故障定位和性能检测功能。在用户信元流中间插入一些有着标准的信元结构的 OAM 信元，可以提供网络的一些特定信息。

ATM OAM 提供了如下功能：

- OAM CC（Continuity Check，连续性检测）检测：一端作为接收端启动 CC 信元的检测功能，一端作为发送端启动 CC 信元的发送功能。如果检测端 3 秒内收不到 CC 信元，PVC 状态变为 DOWN。当再收到 CC 信元后，PVC 状态变为 UP。
- OAM F5 Loopback 检测：用户启动 OAM F5 Loopback 信元的发送以及重传检测功能并指定相关参数后，每隔指定秒发送 OAM F5 Loopback 信元。如果发出 OAM F5 Loopback 信元后在指定秒内未正确收到回应信元，则会立即重发 OAM F5 Loopback 信元。在 OAM F5 Loopback 信元的发送以及重传检测过程中根据收发信元情况更新 PVC 状态。如果 PVC 状态为 DOWN，当连续正确收到指定个 OAM F5 Loopback 信元后，PVC 状态转变为 UP；如果 PVC 状态为 UP，当连续未收到指定个 OAM F5 Loopback 信元后，PVC 状态转变为 DOWN。
- OAM F5 end-to-end 检测：在指定 ATM 接口的特定 PVC 上发送 OAM F5 end-to-end 信元，根据在设定的时间内是否收到应答来判断链路的连接情况。如果规定时间没有收到应答，可能是链路不通，也可能是链路太忙而发生丢包。

1.2 ATM配置限制和指导

仅位于 CMPE-1104、CSPEX-1304S、CSPEX-1404S、CSPEX-1504S、CSPEX-1104-E 单板上的 ATM 接口子卡支持本功能。

1.3 ATM配置任务简介

ATM 配置任务如下：

(1) 配置 ATM 接口

关于 ATM 接口的详细介绍以及相关配置，请参见“接口管理配置指导”中的“ATM 接口”。

(2) 配置 PVC

(3) 配置 ATM 的服务类型

(4) 配置 IPoA 应用

(5) （可选）配置 ATM OAM 功能

1.4 配置PVC

1. 配置限制和指导

在 PVC 方式下，ATM 交换机的交换表项由网管配置，由网管统一分配 VPI/VCI 值，用户根据网管分配的 VPI/VCI 值来配置路由器上的 PVC。如果两台 ATM 设备的 ATM 接口直连，两端 ATM 接口下配置的 VPI/VCI 值必须相同。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 ATM 接口视图或 ATM 子接口视图。

interface atm { *interface-number* | *interface-number.subnumber* }

(3) 创建 PVC 并进入 PVC 视图。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }

(4) 打开当前 PVC。

undo shutdown

缺省情况下，PVC 处于打开状态。

1.5 配置ATM的服务类型

1. 功能简介

ATM 支持四种服务类型：CBR、UBR、VBR-RT、VBR-NRT。用户可以配置 PVC 的服务类型。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 ATM 接口视图或 ATM 子接口视图。

interface atm { *interface-number* | *interface-number.subnumber* }

(3) 进入 PVC 视图

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }

(4) 配置 PVC 的服务类型和相关服务参数。

- 配置 PVC 的服务类型为 CBR，并指定相关的服务参数。

  service cbr *output-pcr* [**cdvt** *cdvt-value*]

- 配置 PVC 的服务类型为 UBR，并指定相关的服务参数。

  service ubr *output-pcr*

- 配置 PVC 的服务类型为 VBR-NRT，并指定相关的服务参数。

  service vbr-nrt *output-pcr output-scr output-mbs*

- 配置 PVC 的服务类型为 VBR-RT，并指定相关的服务参数。

  service vbr-rt *output-pcr output-scr output-mbs*

缺省情况下，PVC 的服务类型为 UBR。

新指定的 PVC 服务类型将会覆盖本 PVC 已有的服务类型，同一个接口下的不同 PVC 可以配置不同的服务类型。

1.6 配置IPoA应用

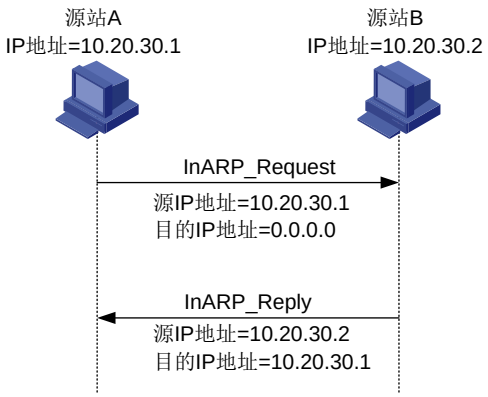
1. IP 地址映射简介

在 ATM 上承载 IP 协议报文时，要想使高层协议能通过对端设备的 IP 地址寻址到对端设备，用户必须将本端的 PVC 与对端设备的 IP 地址关联起来，即配置 PVC 映射的 IP 地址。这样，系统就知道到达某个 IP 地址的报文通过哪个 PVC 进行发送了。

配置 IP 地址映射有三种方法：

- 静态 IP 地址映射：直接指定映射到 PVC 的对端接口的 IP 地址。
- default 映射：配置一个具有缺省路由属性的映射。若某个报文在接口上找不到下一跳地址对应的映射，但某条 PVC 配置了 default 映射，则报文将从该 PVC 上发送。
- InARP 映射：使用 InARP（Inverse Address Resolution Protocol，逆向地址解析协议）来解析与本 PVC 相连的对端接口的 IP 地址，这样不需要为 PVC 静态配置对端的 IP 地址。InARP 交换过程如图 1-4 所示。图中的 IP 地址指的是 PVC 所在 ATM 接口的 IP 地址。

图1-4 InARP 的交换过程



2. 配置限制和指导

- 同一 PVC 只能映射一个 IP 地址，且静态 IP 地址映射、default 映射和 InARP 映射三者同时只能配置其中一个。
- 相同接口下不同的 PVC 不能映射到同一个 IP 地址。
- 同一个接口下的 PVC 最多只能配置一个 default 映射。
- 如果是两台路由器接口直连，本端上映射到对端 IP 地址的 PVC 的 VPI/VCI 值必须和对端上映射到本端 IP 地址的 PVC 的 VPI/VCI 值相同。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 ATM 接口视图或 ATM 子接口视图。

interface atm { *interface-number* | *interface-number.subnumber* }

(3) 进入 PVC 视图。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }

(4) 配置 IPoA 映射，使 PVC 承载 IP 协议报文。

map ip { *ip-address* | **default** | **inarp** [*minutes*] }

缺省情况下，未配置任何映射。

(5) 为 PVC 配置广播属性。

broadcast

缺省情况下，广播属性处于关闭状态。

如果需要在 ATM PVC 上发送广播或者组播报文，请务必配置本命令。

如果某 PVC 配置了广播属性，则 PVC 所属 ATM 接口上的广播或组播报文都要在该 PVC 上发送一份。

1.7 配置ATM OAM功能

1.7.1 开启 ATM OAM 功能

(1) 进入系统视图。

system-view

(2) 进入 ATM 接口视图或 ATM 子接口视图。

interface atm { *interface-number* | *interface-number.subnumber* }

(3) 进入 PVC 视图。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }

(4) 启动 OAM F5 Loopback 信元的发送和重传检测。

oam loopback *interval* [**up** *up-count* **down** *down-count* **retry** *retries*]

缺省情况下，不启动 OAM F5 Loopback 信元的发送，但如果收到 OAM F5 Loopback 信元，则要进行应答。

(5) 启动 OAM CC 功能。

oam cc { both | sink | source }

缺省情况下，OAM CC 功能处于关闭状态。

在配置 OAM CC 功能时，一端配置为 **source**，另一端配置为 **sink**。

1.7.2 检测链路连接情况

可在任意视图下执行本命令，发送 OAM F5 end-to-end 信元，检测链路的连接情况。

oam ping interface atm { *interface-number* | *interface-number.subnumber* } **pvc** { *pvc-name* | *vpi/vci* } [*number timeout*]

1.8 ATM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 ATM 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 PVC 或接口的统计信息。

表1-1 ATM 显示和维护

操作	命令
显示PVC的信息	**display atm pvc-info** [**interface** *interface-type* { *interface-number* | *interface-number.subnumber* } [**pvc** { *pvc-name* | *vpi/vci* }]]
显示PVC的映射信息	**display atm map-info** [**interface** *interface-type* { *interface-number* | *interface-number.subnumber* } [**pvc** { *pvc-name* | *vpi/vci* }]]
清除PVC的统计信息	**reset atm interface** [*interface-type* { *interface-number* | *interface-number.subnumber* }]

1.9 ATM典型配置举例

1.9.1 IPoA 典型配置举例

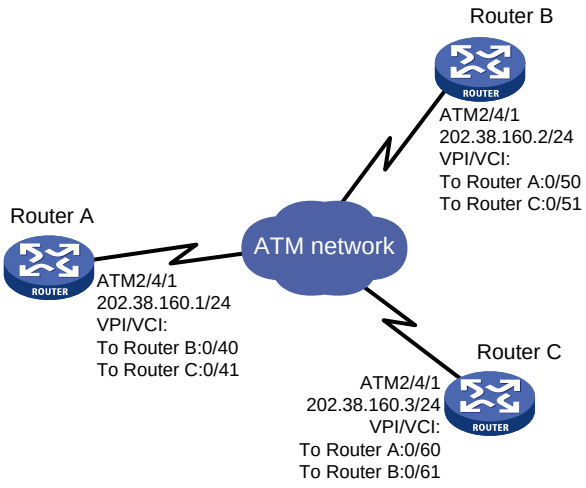
1. 组网需求

Router A、Router B 和 Router C 接入到 ATM 网络中互相通讯。要求：

- 三台路由器 ATM 接口的 IP 地址分别是 202.38.160.1/24、202.38.160.2/24、202.38.160.3/24；
- 在 ATM 网络中，Router A 的 VPI/VCI 是 0/40 和 0/41，分别连接 Router B 和 Router C；Router B 的 VPI/VCI 是 0/50 和 0/51，分别连接 Router A 和 Router C；Router C 的 VPI/VCI 是 0/60 和 0/61，分别连接 Router A 和 Router B；
- 三台路由器的 ATM 接口上的所有 PVC 都采用 IPoA 应用方式。

2. 组网图

图1-5 IPoA 配置组网图



3. 配置步骤

(1) 配置 Router A

进入 ATM 接口，并为其配置 IP 地址。

```
<RouterA> system-view
```

```
[RouterA] interface atm 2/4/1
[RouterA-ATM2/4/1] ip address 202.38.160.1 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[RouterA-ATM2/4/1] pvc to_b 0/40
[RouterA-ATM2/4/1-pvc-to_b-0/40] map ip 202.38.160.2
[RouterA-ATM2/4/1-pvc-to_b-0/40] quit
[RouterA-ATM2/4/1] pvc to_c 0/41
[RouterA-ATM2/4/1-pvc-to_c-0/41] map ip 202.38.160.3
```

(2) 配置 Router B

进入 ATM 接口，并为其配置 IP 地址。

```
<RouterB> system-view
[RouterB] interface atm 2/4/1
[RouterB-ATM2/4/1] ip address 202.38.160.2 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[RouterB-ATM2/4/1] pvc to_a 0/50
[RouterB-ATM2/4/1-pvc-to_a-0/50] map ip 202.38.160.1
[RouterB-ATM2/4/1-pvc-to_a-0/50] quit
[RouterB-ATM2/4/1] pvc to_c 0/51
[RouterB-ATM2/4/1-pvc-to_c-0/51] map ip 202.38.160.3
```

(3) 配置 Router C

进入 ATM 接口，并为其配置 IP 地址。

```
<RouterC> system-view
[RouterC] interface atm 2/4/1
[RouterC-ATM2/4/1] ip address 202.38.160.3 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[RouterC-ATM2/4/1] pvc to_a 0/60
[RouterC-ATM2/4/1-pvc-to_a-0/60] map ip 202.38.160.1
[RouterC-ATM2/4/1-pvc-to_a-0/60] quit
[RouterC-ATM2/4/1] pvc to_b 0/61
[RouterC-ATM2/4/1-pvc-to_b-0/61] map ip 202.38.160.2
```

4. 验证配置

通过此配置，三台路由器之间可以互相 ping 通。

1.10 ATM常见故障处理

1.10.1 采用 IPoA 时，链路状态为 down

1. 故障现象

采用 IPoA 时，链路状态为 down。

2. 故障排除

- 检查光纤是否正确连接。
- 检查本端 IP 地址是否配置。
- 检查是否 PVC 创建失败。

1.10.2 ping 不通对方

1. 故障现象

接口物理层和线路协议都处于 up 状态，但是 **ping** 不通对方。

2. 故障排除

采用 IPoA 时，检查协议地址映射配置是否正确。如果两台路由器的接口直连，本端上映射到对端 IP 地址的 PVC 的（VPI，VCI）必须和对端上映射到本端 IP 地址的 PVC 的（VPI，VCI）相同。

如果两台路由器的接口直连，检查是否有一端的接口时钟设置成了 **master**，应至少有一端的时钟设置成 **master**（内部时钟）；如果路由器接入到 ATM 网络中，传输时钟应当设置为 **slave**（线路时钟）。

检查 ATM 接口，看两端的 ATM 接口是否同为多模光纤接口或单模光纤接口，或者两端使用的是多模光纤接口但使用了单模光纤进行连接。（注意：多数情况下，多模光纤接口和单模光纤接口直接对接是可以互通的，但有时会出现大量丢包和 CRC 错误。）

如果出现 **ping** 小包能通，**ping** 大包不能通的现象，请检查两端路由器接口的 **mtu** 配置是否合适，是否允许大包通过。

1.10.3 ATM 接口状态为 up，但 PVC 状态为 down

1. 故障现象

ATM 接口状态为 up，但 PVC 状态为 down。

2. 故障排除

请检查是否由于启用了 OAM F5 Loopback 信元的发送和重传检测或 OAM CC 检测而导致这种现象。当两台路由器直连时，连接中的 PVC 在这两台设备上的 VPI/VCI 值对必须一致。如果直接连接的对端没有设置与本端相同（即 VPI/VCI 值对一致）的 PVC，则启用了 OAM F5 Loopback 信元的发送和重传检测或 OAM CC 检测后，本端 PVC 的状态无法转变成 up。