H3C SR8800-F 核心路由器

二层技术-广域网接入配置指导

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W732-20160805
产品版本：SR8800-CMW710-R7353P09

前 言

H3C SR8800-F 核心路由器配置指导共分为十六本手册，介绍了 SR8800-F 核心路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《二层技术-广域网接入配置指导》主要介绍了 PPP、HDLC、ATM 等二层广域网链路类型。

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. 端口编号示例约定

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。

产品配套资料

H3C SR8800-F 核心路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	产品彩页	帮助您了解SR8800-F的主要规格参数及亮点
	单板datasheet	帮助您了解SR8800-F的单板属性、特点、支持的标准等
硬件描述与安装	安全兼容性手册	列出SR8800-F的兼容性声明，并对兼容性和安全的细节进行说明
	安装指导	帮助您详细了解SR8800-F的硬件规格和安装方法，指导您对SR8800-F进行安装
	H3C光模块手册	帮助您详细了解SR8800-F设备支持的光模块的类型、外观与规格等内容
业务配置	配置指导	帮助您掌握SR8800-F软件功能的配置方法及配置步骤
	命令参考	详细介绍SR8800-F的命令，相当于命令字典，方便您查阅各个命令的功能
	典型配置举例	帮助您了解产品的典型应用和推荐配置，从组网需求、组网图、配置步骤几方面进行介绍
运行维护	故障处理	帮助您了解在使用SR8800-F过程中碰到困难或者问题的处理方法
	用户FAQ	以问答的形式，帮助您了解SR8800-F的一些软硬件特性及规格等问题
	日志手册	对SR8800-F的系统日志（System Log）消息进行介绍，主要用于指导您理解相关信息的含义，并做出正确的操作
	告警手册	对SR8800-F的告警（Trap）消息进行介绍，主要用于指导您理解相关信息的含义，并做出正确的操作
	MIB Companion	与软件版本配套的MIB Companion
	版本说明书	帮助您了解SR8800-F产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

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和MP

1.1 PPP和MP简介

1.1.1 PPP简介

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

PPP 定义了一整套协议，包括：

- 链路控制协议（Link Control Protocol，LCP）：用来建立、拆除和监控数据链路。
- 网络控制协议（Network Control Protocol，NCP）：用来协商在数据链路上所传输的网络层报文的一些属性和类型。
- 认证协议：用来对用户进行认证，包括 PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）、MS-CHAP（Microsoft CHAP，微软 CHAP 协议）和 MS-CHAP-V2（Microsoft CHAP Version 2）。

1. PPP链路建立过程

PPP链路建立过程如 图 1-1 所示：

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

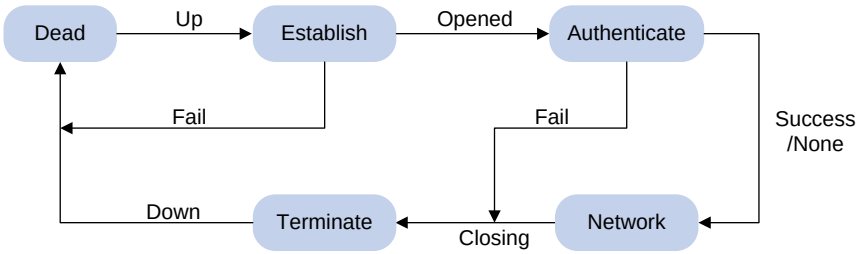
(2) PPP 在 Establish 阶段主要进行 LCP 协商。LCP 协商内容包括：Authentication-Protocol（认证协议类型）、ACCM（Async-Control-Character-Map，异步控制字符映射表）、MRU（Maximum-Receive-Unit，最大接收单元）、Magic-Number（魔术字）、MP（MultiLink PPP，多链路 PPP）等选项。如果 LCP 协商失败，LCP 会上报 Fail 事件，PPP 回到 Dead 状态；如果 LCP 协商成功，LCP 进入 Opened 状态，LCP 会上报 Up 事件，表示链路已经建立（此时对于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

(3) 如果配置了认证，则进入 Authenticate 阶段，开始 PAP、CHAP、MS-CHAP 或 MS-CHAP-V2 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）。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 地址等。）

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

图1-1 PPP 链路建立过程



有关 PPP 的详细介绍请参考 RFC 1661。

2. PPP认证

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

PPP 支持如下认证方式：PAP、CHAP、MS-CHAP、MS-CHAP-V2。

(1) PAP 认证

PAP 为两次握手协议，它通过用户名和密码来对用户进行认证。

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

(2) CHAP 认证

CHAP 为三次握手协议。

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

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

(3) MS-CHAP 认证

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

- MS-CHAP 采用的加密算法是 0x80。
- MS-CHAP 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) MS-CHAP-V2 认证

MS-CHAP-V2 为三次握手协议，认证过程与 CHAP 类似，MS-CHAP-V2 与 CHAP 的不同之处在于：

- MS-CHAP-V2 采用的加密算法是 0x81。
- MS-CHAP-V2 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。
- MS-CHAP-V2 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。
- MS-CHAP-V2 支持修改密码机制。被认证方由于密码过期导致认证失败时，被认证方会将用户输入的新密码信息发回认证方，认证方根据新密码信息重新进行认证。

3. PPP支持IPv4

在 IPv4 网络中，设备在进行 IPCP 协商的过程中可以进行 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 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：若是设备作为 Server 端为 Client 端分配 IP 地址，则应先配置地址池（可以是 PPP 地址池或者 DHCP 地址池），然后在 ISP 域下关联地址池，或者在接口下指定为 Client 端分配的 IP 地址或者地址池，最后再配置 Server 端的 IP 地址，开始进行 IPCP 协商。

当 Client 端配置了 IP 地址可协商属性后，Server 端根据 AAA 认证结果（关于 AAA 的介绍请参见“用户接入配置指导”中的“AAA”）和接口下的配置，按照如下的优先顺序决定是否可以给 Client 端分配 IP 地址：

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

(2) DNS 服务器地址协商

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

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

4. PPP支持IPv6

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

(1) IPv6 地址分配

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

客户端可以通过如下三种方式分配到 IPv6 全球单播地址：

- 方式 1：客户端通过 ND 协议中的 RA 报文获得 IPv6 地址前缀。客户端采用 RA 报文中携带的前缀和 IPv6CP 协商的 IPv6 接口标识一起组合生成 IPv6 全球单播地址。RA 报文中携带的 IPv6 地址前缀的来源有三种：AAA 授权的 IPv6 前缀、接口下配置的 RA 前缀、接口下配置的 IPv6 全球单播地址的前缀。三种来源的优先级依次降低，AAA 授权的优先级最高。关于 ND 协议的详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- 方式 2：客户端通过 DHCPv6 协议申请 IPv6 全球单播地址。在服务器端可以通过 AAA 授权为每个客户端分配不同的地址池，当授权了地址池后，DHCPv6 在分配 IPv6 地址时会从地址池中获取 IPv6 地址分配给客户端。如果 AAA 未授权地址池，DHCPv6 会根据服务器端的 IPv6 地址查找匹配的地址池为客户端分配地址。关于 DHCPv6 协议的详细介绍请参见“用户接入配置指导”中的“DHCPv6”。
- 方式 3：客户端通过 DHCPv6 协议申请代理前缀，客户端通过代理前缀为下面的主机分配 IPv6 全球单播地址。代理前缀分配方式中地址池的选择原则和通过 DHCPv6 协议分配 IPv6 全球单播地址方式中地址池的选择原则一致。

根据组网不同，主机获取 IPv6 地址的方式如下：

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

(2) IPv6 DNS 服务器地址分配

在 IPv6 网络中，IPv6 DNS 服务器地址的分配有如下两种方式：

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

1.1.2 MP简介

MP（MultiLink PPP，多链路 PPP）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。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。

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

MP 能在支持 PPP 封装的接口（除 POS 接口）下工作，如串口，也包括支持 PPPoX（如 PPPoE 等）的虚拟接口，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。

1.2 配置PPP

1.2.1 PPP配置任务简介

表1-1 PPP 配置任务简介

配置任务	说明	详细配置
配置接口封装PPP协议	必选	1.2.2
配置PPP认证方式	可选	1.2.3
配置轮询时间间隔	可选	1.2.4
配置PPP协商参数	可选	1.2.5
配置PPP计费统计功能	可选	1.2.6
配置PPP接入用户日志信息功能	可选	1.2.7
配置业务跟踪对象功能	可选	1.2.8
配置PPP用户的nas-port-type属性	可选	1.2.9

1.2.2 配置接口封装PPP协议

表1-2 配置接口封装 PPP 协议

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口封装的链路层协议为PPP	**link-protocol ppp**	缺省情况下，串口、POS接口的链路层协议为PPP

1.2.3 配置PPP认证方式

PPP 支持如下认证方式：PAP、CHAP、MS-CHAP、MS-CHAP-V2。用户可以同时配置多种认证方式，在 LCP 协商过程中，认证方根据用户配置的认证方式顺序逐一与被认证方进行协商，直到协商通过。如果协商过程中，被认证方回应的协商报文中携带了建议使用的认证方式，认证方查找配置中存在该认证方式，则直接使用该认证方式进行认证。

1. 配置PAP认证

(1) 配置认证方

表1-3 配置认证方

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

(2) 配置被认证方

表1-4 配置被认证方

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

2. 配置CHAP认证

CHAP 认证分为两种：认证方配置了用户名和认证方没有配置用户名。

(1) 认证方配置了用户名

- 配置认证方

表1-5 配置认证方

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

- 配置被认证方

表1-6 配置被认证方

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

(2) 认证方没有配置用户名

- 配置认证方

表1-7 配置认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为CHAP	**ppp authentication-mode chap** [[**call-in**] **domain** { *isp-name* | **default enable** *isp-name* }]	缺省情况下，PPP协议不进行认证

操作	命令	说明
配置本地AAA认证或者远程AAA认证	请参见“用户接入配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名必须与被认证方上的配置一致 为被认证方配置的密码必须与被认证方上配置的CHAP认证密码一致

- 配置被认证方

表1-8 配置被认证方

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置采用CHAP认证时被认证方的用户名	**ppp chap user** *username*	缺省情况下，CHAP认证的用户名为空 在认证方上为被认证方配置的用户名必须跟此处配置的一致
设置CHAP认证密码	**ppp chap password** { **cipher** | **simple** } *password*	缺省情况下，没有配置进行CHAP认证时采用的密码 在认证方上为被认证方配置的密码必须跟此处配置的一致

3. 配置MS-CHAP或MS-CHAP-V2 认证

与 CHAP 认证相同，MS-CHAP 和 MS-CHAP-V2 认证也分为两种：认证方配置了用户名和认证方没有配置用户名。

配置 MS-CHAP 或 MS-CHAP-V2 认证时需注意：

- 设备只能作为 MS-CHAP 和 MS-CHAP-V2 的认证方来对其它设备进行认证。
- L2TP 环境下仅支持 MS-CHAP 认证，不支持 MS-CHAP-V2 认证。
- MS-CHAP-V2 认证只有在 RADIUS 认证的方式下，才能支持修改密码机制。

表1-9 配置 MS-CHAP 或 MS-CHAP-V2 认证的认证方（认证方配置了用户名）

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为MS-CHAP或MS-CHAP-V2	**ppp authentication-mode** { **ms-chap** | **ms-chap-v2** } [[**call-in**] **domain** { *isp-name* | **default enable** *isp-name* }]	缺省情况下，PPP协议不进行认证
配置采用MS-CHAP或MS-CHAP-V2认证时认证方的用户名	**ppp chap user** *username*	在被认证方上为认证方配置的用户名必须跟此处配置的一致
配置本地AAA认证或者远程AAA认证	请参见“用户接入配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名和密码必须与被认证方上的配置一致

表1-10 配置 MS-CHAP 或 MS-CHAP-V2 认证的认证方（认证方没有配置用户名）

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置本地认证对端的方式为MS-CHAP或MS-CHAP-V2	**ppp authentication-mode** { **ms-chap** | **ms-chap-v2** } [[**call-in**] **domain** { *isp-name* | **default enable** *isp-name* }]	缺省情况下，PPP协议不进行认证
配置本地AAA认证或者远程AAA认证	请参见“用户接入配置指导”中的“AAA” • 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码 • 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码	为被认证方配置的用户名和密码必须与被认证方上的配置一致

1.2.4 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。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。如果接口在 3 个 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。

用户可以通过 **timer-hold** 命令修改 keepalive 报文轮询的时间间隔。如果将轮询时间间隔配置为 0 秒，则不发送 keepalive 报文。

在速率非常低的链路上，轮询时间间隔不能配置过小。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 3 个 keepalive 周期之后仍然无法收到对端的 keepalive 报文，它就会认为链路发生故障。如果 keepalive 报文被延迟的时间超过接口的这个限制，链路就会被认为发生故障而被关闭。

表1-11 配置轮询时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置轮询时间间隔	**timer-hold** *period*	缺省情况下，POS接口和Serial接口的轮询时间间隔为10秒；虚拟模板接口的轮询时间间隔为20秒。

1.2.5 配置PPP协商参数

可以配置的 PPP 协商参数包括：

- 协商超时时间间隔
- 协商 IP 地址

1. 配置协商超时时间间隔

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

表1-12 配置协商超时时间间隔

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
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

2. 配置PPP协商IP地址

设备在进行 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 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：若是设备作为 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，或者在接口下指定为 Client 端分配的 IP 地址或者地址池，最后再配置 Server 端的 IP 地址，开始进行 IPCP 协商。

当 Client 端配置了 IP 地址可协商属性后，Server 端根据 AAA 认证结果和接口下的配置，按照如下的优先顺序决定是否可以给 Client 端分配 IP 地址：

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

(1) 配置 Client 端

表1-13 配置 Client 端

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

(2) 配置 Server 端

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

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

这三种方式中，不同 PPP 用户可以采用的方式如下：

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

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

表1-14 配置 Server 端（在接口下指定为 Client 端分配的 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口为Client端分配的IP地址	**remote address** *ip-address*	缺省情况下，接口不为Client端分配IP地址
配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址
（可选）使能接口的IP网段检查功能	**ppp ipcp remote-address match**	缺省情况下,没有配置接口的IP网段检查功能

表1-15 配置 Server 端（从接口下指定的 PPP 地址池中为 Client 端分配 IP 地址）

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

表1-16 配置 Server 端（从接口下指定的 DHCP 地址池中为 Client 端分配 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
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、DHCP 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 DHCP 地址池	DHCP的具体配置介绍请参见“用户接入配置指导”中的“DHCP”
进入接口视图	**interface** *interface-type interface-number*	-
使用DHCP地址池为Client端分配IP地址	**remote address pool** *pool-name*	缺省情况下，接口不为Client端分配IP地址
配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址
（可选）使能接口的IP网段检查功能	**ppp ipcp remote-address match**	缺省情况下，没有配置接口的IP网段检查功能

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

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

表1-18 配置 Server 端（从 ISP 域下关联的 DHCP 地址池中分配 IP 地址）

操作	命令	说明
进入系统视图	**system-view**	-
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、DHCP 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 DHCP 地址池	DHCP的具体配置介绍请参见“用户接入配置指导”中的“DHCP”
进入ISP域视图	**domain** *isp-name*	-
在ISP域下关联DHCP地址池为Client端分配IP地址	**authorization-attribute ip-pool** *pool-name*	缺省情况下，ISP域下没有关联DHCP地址池 本命令的详细介绍请参见“用户接入命令参考”中的“AAA”
退回系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置Server端的IP地址	**ip address** *ip-address*	缺省情况下，接口没有配置IP地址

3. 配置DNS服务器地址协商

(1) 配置 Client 端

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

表1-19 配置 Client 端

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

(2) 配置 Server 端

表1-20 配置 Server 端

操作	命令	说明
进入系统视图	**system-view**	-
进入虚拟模板接口视图	**interface virtual-template** *number*	-

操作	命令	说明
配置设备为对端设备指定DNS服务器地址	**ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]	缺省情况下，设备不为对端设备指定DNS服务器的IP地址 收到Client端的请求后，Server端才会为对端指定DNS服务器地址

1.2.6 配置PPP计费统计功能

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

表1-21 配置 PPP 计费统计功能

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

1.2.7 配置PPP接入用户日志功能

PPP 接入用户日志是为了满足网络管理员维护的需要，对用户的上线、下线、上线失败的信息进行记录，包括用户名、IP 地址、接口名称、两层 VLAN、MAC 地址、上线失败原因、下线原因等。设备生成的 PPP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

为了防止设备输出过多的 PPP 日志信息，一般情况下建议不要开启此功能。

表1-22 配置 PPP 接入用户日志信息功能

操作	命令	说明
进入系统视图	**system-view**	-
开启PPP接入用户日志功能	**ppp access-user log enable** [**successful-login** | **failed-login** | **normal-logout** | **abnormal-logout**] *	缺省情况下，PPP接入用户日志功能处于关闭状态

1.2.8 配置业务跟踪对象功能

业务跟踪对象功能是为了满足网络管理员维护的需要，管理员可以通过创建业务追踪对象可以追踪接入用户的上下线相关信息的，通过指定不同的匹配参数，可以实现对特定用户的追踪。

开启本功能会时占用大量系统资源，建议仅在故障诊断时使用，一般情况下不要使用。

需要注意的是，主备倒换后业务跟踪对象配置会自动失效，需要重新配置。

表1-23 配置业务跟踪对象功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置业务跟踪对象功能	**trace access-user object** *object-id* { **access-mode pppoe** | **username** *user-name* | **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **c-vlan** *vlan-id* | **s-vlan** *vlan-id* } * [**output** { **file** *file-name* | **syslog-server** *server-ip-address* | **vty** } | **aging** *time*] *	缺省情况下，不存在业务跟踪对象

1.2.9 配置PPP用户的nas-port-type属性

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

表1-24 配置 PPP 用户的 nas-port-type 属性

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

1.3 配置MP

说明

- 不支持跨单板进行 MP 捆绑。仅支持同一接口子卡内的接口进行 MP 捆绑，不支持同一业务板上跨接口子卡进行 MP 捆绑。
- 仅 MIC-ET16L、MIC-CLP2L 和 MIC-CLP4L 子卡支持 MP 捆绑。

1.3.1 MP配置任务简介

设备通过 MP-group 接口来配置 MP。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。MP-group 接口配置方式快速高效、配置简单、容易理解。

表1-25 MP 配置任务简介

配置任务	说明	详细配置
通过MP-group接口配置MP	必选	1.3.2
配置MP短序协商方式	可选	1.3.3

配置任务	说明	详细配置
配置MP Endpoint选项	可选	1.3.4

1.3.2 通过MP-group接口配置MP

表1-26 通过 MP-group 接口配置 MP

操作	命令	说明
进入系统视图	**system-view**	-
创建MP-group接口并进入指定的MP-group接口视图	**interface mp-group** *mp-number*	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
（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16 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
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
（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
（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 配置**ppp mp fragment disable**命令后，接口的**ppp mp min-fragment**命令不再起作用
（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 Interface
配置轮询时间间隔	**timer-hold** *period*	缺省情况下，轮询时间间隔为10秒
配置接口的MTU值	**mtu** *size*	缺省情况下，接口的MTU值为1500字节
（可选）恢复接口的缺省配置	**default**	-
配置MP使用严格负载分担模式	**ppp mp load-sharing mode strict-round-robin**	可选 缺省情况下，MP使用智能负载分担模式
打开接口	**undo shutdown**	缺省情况下，接口处于打开状态
退回系统视图	**quit**	-
进入Serial接口视图	**interface Serial** *interface-number*	-
将串口加入指定的MP-group接口，使接口工作在MP方式	**ppp mp mp-group** *mp-number*	缺省情况下，串口工作在普通PPP方式

1.3.3 配置MP短序协商方式

MP 捆绑组在收发报文时默认使用长序方式（长序、短序是指报文序号的长短）。

配置本功能时需要注意：

- 如果本端接收使用短序，则需要在协商 LCP 的过程添加短序请求，请求对端发送短序，协商通过后，对端使用短序发送。

- 如果本端发送使用短序，则需要对端发出短序协商请求，协商通过后，本端使用短序发送。
- MP 捆绑组使用的长短序方式由第一条加入该捆绑组中的子通道决定，后续加入捆绑组的子通道配置不能更改 MP 捆绑组的长短序方式。
- 如果想使用 MP 短序协商，对于普通 MP（即非拨号 MP），建议在所有的 MP 子通道下配置该命令。配置该命令会导致 PPP 重协商。

表1-27 配置 MP 短序协商方式

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
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

1.3.4 配置MP Endpoint选项

在 MP 的 LCP 协商过程会协商 Endpoint 选项（终端描述符）值：

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 字符，如果内容超过 20 个字符，则截取前 20 个字符作为 Endpoint 选项内容。

表1-28 配置 MP Endpoint 选项

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置当前接口在MP应用时，LCP协商的Endpoint选项内容	**ppp mp endpoint** *endpoint*	-

1.4 PPP和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 PPP 和 MP 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除相应接口的统计信息。

表1-29 PPP 和 MP 显示和维护

操作	命令
显示地址池的信息	**display ip pool** [*pool-name* | **group** *group-name*]
显示接入用户的信息（独立运行模式）	**display ppp access-user** { **domain** *domain-name* [**count** | **verbose**] | **interface** *interface-type interface-number* [**count** | **verbose**] | **ip-address** *ipv4-address* | **ipv6-address** *ipv6-address* | **ip-type** { **ipv4 | ipv6 | dual-stack** } [**count** | **verbose**] | **mac-address** *mac-address* | **pool** *pool-name* [**count** | **verbose**] | **s-vlan** *svlan-minimum* [*svlan-maximum*] [**c-vlan** *cvlan-minimum* [*cvlan-maximum*]] [**count** | **verbose**] | **username** *user-name* | **user-type** { **lac** | **lns** | **pppoa** | **pppoe** } [**count | verbose**] | **vpn-instance** *vpn-name* [**count** | **verbose**] } [**slot** *slot-number*]

操作	命令
显示接入用户的信息（IRF模式）	**display ppp access-user** { **domain** *domain-name* [**count** | **verbose**] | **interface** *interface-type interface-number* [**count** | **verbose**] | **ip-address** *ipv4-address* | **ipv6-address** *ipv6-address* | **ip-type** { **ipv4 | ipv6 | dual-stack** } [**count** | **verbose**] | **mac-address** *mac-address* | **pool** *pool-name* [**count** | **verbose**] | **s-vlan** *svlan-minimum* [*svlan-maximum*] [**c-vlan** *cvlan-minimum* [*cvlan-maximum*]] [**count** | **verbose**] | **username** *user-name* | **user-type** { **lac** | **lns** | **pppoa** | **pppoe** } [**count | verbose**] | **vpn-instance** *vpn-name* [**count** | **verbose**] } [**chassis** *chassis-number* **slot** *slot-number*]
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*]
显示PPP的协商报文统计信息（IRF模式）	**display ppp packet statistics** [**chassis** *chassis-number* **slot** *slot-number*]
显示虚拟模板接口的相关信息	**display interface** [**virtual-template** [*interface-number*]] [**brief** [**description** | **down**]]
显示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*]
使指定用户下线（独立运行模式）	**reset ppp access-user** { **domain** *domain-name* | **interface** *interface-type interface-number* | **ip-address** *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] **| ipv6-address** *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] **| ip-type** { **ipv4 | ipv6 | dual-stack** } | **mac-address** *mac-address* | **pool** *pool-name* | **s-vlan** *svlan-minimum* [*svlan-maximum*] [**c-vlan** *cvlan-minimum* [*cvlan-maximum*]] | **username** *user-name* | **user-type** { **lac** | **lns** | **pppoa** | **pppoe** } | **vpn-instance** *vpn-name* } [**slot** *slot-number*]
使指定用户下线（IRF模式）	**reset ppp access-user** { **domain** *domain-name* | **interface** *interface-type interface-number* | **ip-address** *ipv4-address* [**vpn-instance** *ipv4-vpn-instance-name*] **| ipv6-address** *ipv6-address* [**vpn-instance** *ipv6-vpn-instance-name*] **| ip-type** { **ipv4 | ipv6 | dual-stack** } | **mac-address** *mac-address* | **pool** *pool-name* | **s-vlan** *svlan-minimum* [*svlan-maximum*] [**c-vlan** *cvlan-minimum* [*cvlan-maximum*]] | **username** *user-name* | **user-type** { **lac** | **lns** | **pppoa** | **pppoe** } | **vpn-instance** *vpn-name* } [**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*]
清除PPP的协商报文统计信息（IRF模式）	**reset ppp packet statistics** [**chassis** *chassis-number* **slot** *slot-number*]
清除MP-group接口的统计信息	**reset counters interface** [**mp-group** [*interface-number*]]

1.5 PPP和MP典型配置举例

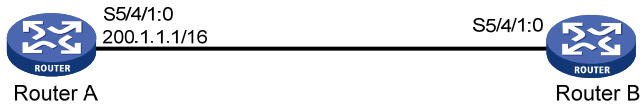
1.5.1 PAP单向认证举例

1. 组网需求

如 图 1-2 所示，Router A和Router B之间用接口Serial5/4/1:0 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 passb
```

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 5/4/1:0
[RouterA-Serial5/4/1:0] link-protocol ppp
```

配置本地认证 Router B 的方式为 PAP。

```
[RouterA-Serial5/4/1:0] ppp authentication-mode pap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial5/4/1:0] ip address 200.1.1.1 16
[RouterA-Serial5/4/1:0] 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 system
[RouterA-isp-system] authentication ppp local
```

(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 5/4/1:0
[RouterB-Serial5/4/1:0] 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-Serial5/4/1:0] ppp pap local-user userb password simple passb
```

配置接口的 IP 地址。

```
[RouterB-Serial5/4/1:0] ip address 200.1.1.2 16
```

4. 验证配置

通过 **display interface serial** 命令，查看接口 Serial5/4/1:0 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-Serial5/4/1:0] display interface serial 5/4/1:0
Serial5/4/1:0
Current state: UP
Line protocol state: UP
Description: Serial5/4/1:0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
```

```
Internet Address: 200.1.1.2/16 Primary
Link layer protocol: PPP
LCP: opened, IPCP: opened
…略…
[RouterB-Serial5/4/1:0] 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
```

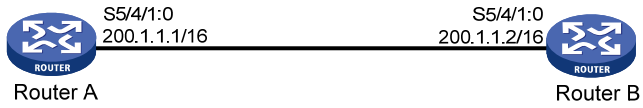
1.5.2 PAP双向认证举例

1. 组网需求

如 图 1-3 所示，Router A和Router B之间用接口Serial5/4/1:0 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 passb
```

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 5/4/1:0
[RouterA-Serial5/4/1:0] link-protocol ppp
```

配置本地认证 Router B 的方式为 PAP。

```
[RouterA-Serial5/4/1:0] 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-Serial5/4/1:0] ppp pap local-user usera password simple passa
```

配置接口的 IP 地址。

```
[RouterA-Serial5/4/1:0] ip address 200.1.1.1 16
[RouterA-Serial5/4/1:0] 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 system
```

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

(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 passa
```

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 5/4/1:0
[RouterB-Serial5/4/1:0] link-protocol ppp
```

配置本地认证 Router A 的方式为 PAP。

```
[RouterB-Serial5/4/1:0] 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-Serial5/4/1:0] ppp pap local-user userb password simple passb
```

配置接口的 IP 地址。

```
[RouterB-Serial5/4/1:0] ip address 200.1.1.2 16
[RouterB-Serial5/4/1:0] 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 system
[RouterB-isp-system] authentication ppp local
```

4. 验证配置

通过 **display interface serial** 命令，查看接口 Serial5/4/1:0 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-isp-system] display interface serial 5/4/1:0
Serial5/4/1:0
Current state: UP
Line protocol state: UP
Description: Serial5/4/1:0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Internet Address: 200.1.1.2/16 Primary
Link layer protocol: PPP
LCP opened, IPCP opened
…略…
[RouterB-isp-system] 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
```

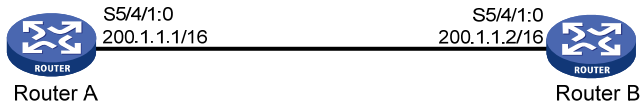
1.5.3 CHAP单向认证举例

1. 组网需求

在 图 1-2 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 hello
```

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 5/4/1:0
[RouterA-Serial5/4/1:0] link-protocol ppp
```

配置采用 CHAP 认证时 Router A 的用户名。

```
[RouterA-Serial5/4/1:0] ppp chap user usera
```

配置本地认证 Router B 的方式为 CHAP。

```
[RouterA-Serial5/4/1:0] ppp authentication-mode chap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial5/4/1:0] ip address 200.1.1.1 16
[RouterA-Serial5/4/1:0] 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 system
[RouterA-isp-system] authentication ppp local
```

(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 hello
```

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 5/4/1:0
[RouterB-Serial5/4/1:0] link-protocol ppp
```

配置采用 CHAP 认证时 Router B 的用户名。

```
[RouterB-Serial5/4/1:0] ppp chap user userb
```

配置接口的 IP 地址。

```
[RouterB-Serial5/4/1:0] ip address 200.1.1.2 16
```

4. 配置方法二（以CHAP方式认证对端时，认证方没有配置用户名）

(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 hello
```

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 5/4/1:0
[RouterA-Serial5/4/1:0] ppp authentication-mode chap domain system
```

配置接口的 IP 地址。

```
[RouterA-Serial5/4/1:0] ip address 200.1.1.1 16
[RouterA-Serial5/4/1:0] 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 system
[RouterA-isp-system] authentication ppp local
```

(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 5/4/1:0
[RouterB-Serial5/4/1:0] ppp chap user userb
```

设置缺省的 CHAP 认证密码。

```
[RouterB-Serial5/4/1:0] ppp chap password simple hello
```

配置接口的 IP 地址。

```
[RouterB-Serial5/4/1:0] ip address 200.1.1.2 16
```

5. 验证配置

通过 **display interface serial** 命令，查看接口 Serial5/4/1:0 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-Serial5/4/1:0] display interface serial 5/4/1:0
Serial5/4/1:0
Current state: UP
Line protocol state: UP
Description: Serial5/4/1:0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Internet Address: 200.1.1.2/16 Primary
Link layer protocol: PPP
LCP opened, IPCP opened
…略…
[RouterB-Serial5/4/1:0] 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
```

1.5.4 IP地址协商举例一（在接口下指定为Client端分配的IP地址）

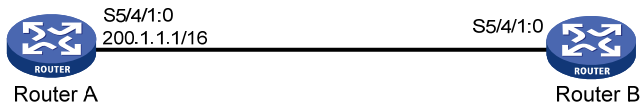
1. 组网需求

Router A 通过 PPP 协商，为 Router B 的接口 Serial5/4/1:0 分配 IP 地址。

要求 Router A 用接口下指定的 IP 地址为 Router B 分配 IP 地址。

2. 组网图

图1-5 配置 IP 地址协商组网图



3. 配置步骤

(1) 配置 Router A

配置接口 Serial5/4/1:0 为 Router B 的接口分配的 IP 地址。

```
<RouterA> system-view
[RouterA] interface serial 5/4/1:0
[RouterA-Serial5/4/1:0] remote address 200.1.1.10
```

配置接口 Serial5/4/1:0 的 IP 地址。

```
[RouterA-Serial5/4/1:0] ip address 200.1.1.1 16
```

(2) 配置 Router B

配置接口 Serial5/4/1:0 通过协商获取 IP 地址。

```
<RouterB> system-view
[RouterB] interface serial 5/4/1:0
[RouterB-Serial5/4/1:0] ip address ppp-negotiate
```

4. 验证配置

配置完成后，查看设备 Router B 的接口 Serial5/4/1:0 的概要信息，可见接口 Serial5/4/1:0 通过 PPP 协商获取的 IP 地址为 200.1.1.10。

```
[RouterB-Serial5/4/1:0] display interface serial 5/4/1:0 brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
S5/4/1:0             UP   UP       200.1.1.10
```

在 Router B 上可以 Ping 通 Router A 的 Serial5/4/1:0 接口。

```
[RouterB-Serial5/4/1:0] 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
```

1.5.5 IP地址协商举例二（从接口下指定的PPP地址池中分配IP地址）

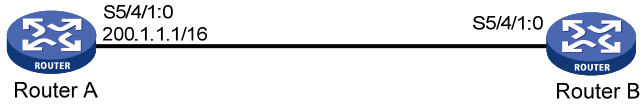
1. 组网需求

Router A 通过 PPP 协商，为 Router B 的接口 Serial5/4/1:0 分配 IP 地址。

要求 Router A 从接口下指定的 PPP 地址池中分配 IP 地址。

2. 组网图

图1-6 配置 IP 地址协商组网图



3. 配置步骤

(1) 配置 Router A

配置 PPP 地址池 aaa，IP 地址范围为 200.1.1.10 到 200.1.1.20，PPP 地址池所在的组为 AAA。

```
<RouterA> system-view
[RouterA] ip pool aaa 200.1.1.10 200.1.1.20 group AAA
```

配置接口 Serial5/4/1:0 使用 PPP 地址池为 Router B 的接口分配 IP 地址。

```
[RouterA] interface serial 5/4/1:0
[RouterA-Serial5/4/1:0] remote address pool aaa
```

配置接口 Serial5/4/1:0 的 IP 地址。

```
[RouterA-Serial5/4/1:0] ip address 200.1.1.1 16
```

(2) 配置 Router B

配置接口 Serial5/4/1:0 通过协商获取 IP 地址。

```
<RouterB> system-view
[RouterB] interface serial 5/4/1:0
[RouterB-Serial5/4/1:0] ip address ppp-negotiate
```

4. 验证配置

配置完成后，查看设备 Router B 的接口 Serial5/4/1:0 的概要信息，可见接口 Serial5/4/1:0 通过 PPP 协商获取的 IP 地址为 200.1.1.10。

```
[RouterB-Serial5/4/1:0] display interface serial 5/4/1:0 brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
S5/4/1:0             UP   UP       200.1.1.10
```

在 Router B 上可以 Ping 通 Router A 的 Serial5/4/1:0 接口。

```
[RouterB-Serial5/4/1:0] 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 PPP 地址池中已分配一个地址。

```
[RouterA-Serial5/4/1:0] display ip pool aaa
Group name: AAA
  Pool name       Start IP address    End IP address     Free    In use
  aaa             200.1.1.10          200.1.1.20         10      1

In use IP addresses:
  IP address      Interface
  200.1.1.10      S5/4/1:0
```

1.5.6 IP地址协商举例三（从ISP域下关联的PPP地址池中分配IP地址）

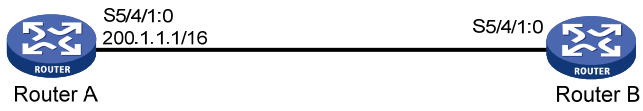
1. 组网需求

Router A 通过 PPP 协商，为 Router B 的接口 Serial5/4/1:0 分配 IP 地址。

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

2. 组网图

图1-7 配置 IP 地址协商组网图



3. 配置步骤

(1) 配置 Router A

配置 PPP 地址池 aaa，IP 地址范围为 200.1.1.10 到 200.1.1.20，PPP 地址池所在的组为 AAA。

```
<RouterA> system-view
[RouterA] ip pool aaa 200.1.1.10 200.1.1.20 group AAA
```

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 123
```

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 PPP 地址池。

```
[RouterA] domain bbb
[RouterA-isp-bbb] authorization-attribute ip-pool aaa
[RouterA-isp-bbb] quit
```

配置接口 Serial5/4/1:0 在 ISP 域 bbb 中采用 PAP 方式认证 Router B。

```
[RouterA] interface serial 5/4/1:0
[RouterA-Serial5/4/1:0] ppp authentication-mode pap domain bbb
```

配置接口 Serial5/4/1:0 的 IP 地址。

```
[RouterA-Serial5/4/1:0] ip address 200.1.1.1 16
```

(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 5/4/1:0
[RouterB-Serial5/4/1:0] ppp pap local-user usrb password simple 123
```

配置接口 Serial5/4/1:0 通过协商获取 IP 地址。

```
[RouterB-Serial5/4/1:0] ip address ppp-negotiate
```

4. 验证配置

配置完成后，查看设备 Router B 的接口 Serial5/4/1:0 的概要信息，可见接口 Serial5/4/1:0 通过 PPP 协商获取的 IP 地址为 200.1.1.10。

```
[RouterB-Serial5/4/1:0] display interface serial 5/4/1:0 brief
Brief information on interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
S5/4/1:0             UP   UP       200.1.1.10
```

在 Router B 上可以 Ping 通 Router A 的 Serial5/4/1:0 接口。

```
[RouterB-Serial5/4/1:0] 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 PPP 地址池中已分配一个地址。

```
[RouterA-Serial5/4/1:0] display ip pool
Group name: AAA
  Pool name       Start IP address    End IP address     Free     In use
  aaa             200.1.1.10          200.1.1.20         10       1
In use IP addresses:
  IP address      Interface
  200.1.1.10      S5/4/1:0
```

1.5.7 MP配置举例

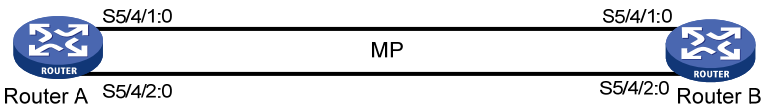
1. 组网需求

设备 Router A 和 Router B 的 Serial5/4/2:0 和 Serial5/4/1:0 分别对应连接。

要求采用 MP-group 接口实现 MP。

2. 组网图

图1-8 MP 配置组网图



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 5/4/1
[RouterA-Mp-group5/4/1] ip address 1.1.1.1 24
```

配置串口 Serial5/4/2:0。

```
[RouterA-Mp-group5/4/1] quit
[RouterA] interface serial 5/4/2:0
[RouterA-Serial5/4/2：0] link-protocol ppp
[RouterA-Serial5/4/2：0] ppp mp mp-group 5/4/1
[RouterA-Serial5/4/2：0] shutdown
[RouterA-Serial5/4/2：0] undo shutdown
[RouterA-Serial5/4/2：0] quit
```

配置串口 Serial5/4/1:0。

```
[RouterA] interface serial 5/4/1:0
[RouterA-Serial5/4/1：0] link-protocol ppp
[RouterA-Serial5/4/1：0] ppp mp mp-group 5/4/1
[RouterA-Serial5/4/1：0] shutdown
[RouterA-Serial5/4/1：0] undo shutdown
[RouterA-Serial5/4/1：0] quit
```

(2) 配置 Router B

创建 MP-group 接口，配置相应的 IP 地址。

```
[RouterB] interface mp-group 5/4/1
[RouterB-Mp-group5/4/1] ip address 1.1.1.2 24
[RouterB-Mp-group5/4/1] quit
```

配置串口 Serial5/4/2:0。

```
[RouterB] interface serial 5/4/2:0
[RouterB-Serial5/4/2：0] link-protocol ppp
 [RouterB-Serial5/4/2：0] ppp mp mp-group 5/4/1
[RouterB-Serial5/4/2：0] shutdown
[RouterB-Serial5/4/2：0] undo shutdown
[RouterB-Serial5/4/2：0] quit
```

配置串口 Serial5/4/1:0。

```
[RouterB] interface serial 5/4/1:0
[RouterB-Serial5/4/1：0] link-protocol ppp
[RouterB-Serial5/4/1：0] ppp mp mp-group 5/4/1
[RouterB-Serial5/4/1：0] shutdown
[RouterB-Serial5/4/1：0] undo shutdown
[RouterB-Serial5/4/1：0] quit
```

(3) 在 Router A 上查看绑定效果

查看 MP 的相关信息。

```
[RouterA] display ppp mp
Template: Mp-group5/4/1
max-bind: 16, fragment: enabled, min-fragment: 128
Master link: MP-group5/4/1, Active members: 2, Bundle Multilink
Peer's endPoint descriptor: Mp-group5/4/1
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
      Serial5/4/2：0              Up-Time:2012/11/04  09:03:16:613
```

```
      Serial5/4/1：0               Up-Time:2012/11/04  09:03:42:945
```

查看 Mp-group5/4/1 接口的相关信息。

```
[RouterA] display interface mp-group 5/4/1
Mp-group5/4/1
Current state: UP
Line protocol state: UP
Description: Mp-group5/4/1 Interface
Bandwidth: 0kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 1.1.1.1/24 Primary
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened
Physical: MP
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

说明

设备支持两种运行模式：独立运行模式和 IRF 模式，缺省情况为独立运行模式。有关 IRF 模式的介绍，请参见“虚拟化技术配置指导”中的“IRF”。

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，均可以实现透明的传输。

- 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，如果是同/异步串口的话，只有当同/异步串口工作在同步模式下才可以应用 HDLC 协议。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。

1.2 配置接口封装HDLC协议

表1-1 配置接口封装 HDLC 协议

操作	命令	说明
进入系统视图	**system-view**	-
进入同步模式的Serial接口或POS接口视图	**interface** *interface-type interface-number*	-
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 配置轮询时间间隔

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（发送周期为 **timer-hold** 命令配置的轮询时间间隔）， 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。当接口收到对端发来的、携带有本端前一次发送序号的 keepalive 报文后，接口下次发送的 keepalive 报文中的发送序号将加一，否则发送序号不变。如果接口在 5 个轮询时间间隔内无法收到对端发来的、携带有本端前一次发送序号的 keepalive 报文，链路层会认为对端故障，上报链路层 down。

配置轮询时间间隔时需要注意：

- 如果将轮询时间间隔配置为 0 秒，则不发送 keepalive 报文。
- 在配置轮询时间间隔时，建议链路两端的设置保持一致。
- 如果网络的延迟比较大，或拥塞程度较高，可以适当加大轮询时间的间隔，以避免链路被认为发生故障而被关闭。

表1-2 配置轮询时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置轮询时间间隔	**timer-hold** *seconds*	缺省情况下，接口的轮询时间间隔为10秒

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1-3 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*]]

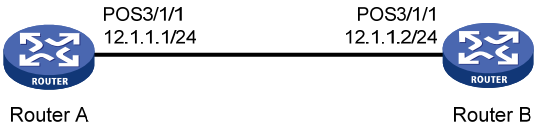
1.5 HDLC典型配置举例

1. 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。

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。

2.1.1 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，只有物理 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。

2.1.2 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

级和接口索引号来为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。

2.1.3 负载分担方式

HDLC 捆绑是通过选中成员接口来转发流量的。当 HDLC 捆绑中存在多个选中成员接口时，设备会根据负载分担方式来选择选中成员接口发送流量。负载分担方式分为逐流负载分担和逐包负载分担两种，原理如下：

- 逐流负载分担：通过源 IP 地址和目的 IP 地址等将报文分成不同的流，同一条流的报文将在同一个选中成员接口上发送。目前支持 IPv4、IPv6 报文根据源 IP 地址和目的 IP 地址进行分流（源 IP 地址和目的 IP 地址都相同的报文，属于同一条流），MPLS 报文根据标签进行分流。
- 逐包负载分担：以报文为单位，将流量分担到不同的选中成员接口上进行发送。

说明

目前，设备仅支持逐流负载分担。

2.2 配置HDLC捆绑接口

配置 HDLC 捆绑接口时需要注意：

- 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。
- 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。
- 建议 HDLC 捆绑链路两端采用相同的负载分担方式。

表2-1 配置 HDLC 捆绑接口

操作	命令	说明
进入系统视图	**system-view**	-
创建HDLC捆绑接口并进入HDLC捆绑接口视图	**interface hdlc-bundle** *bundle-id*	缺省情况下，不存在HDLC捆绑接口
（可选）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
（可选）配置最多选中成员接口数目	**bundle max-active links** *number*	缺省情况下，设备支持的最多选中成员接口数目为8

操作	命令	说明
（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
（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”
（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
（可选）恢复HDLC捆绑接口的缺省配置	**default**	-
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

2.3 配置接口加入HDLC捆绑

配置接口加入 HDLC 捆绑时需要注意：

- 只有物理 POS 接口可以加入 HDLC 捆绑。
- 配置了下列功能的 POS 接口不能加入 HDLC 捆绑：配置 IPv4 地址和地址借用的 POS 接口、配置 IPv6 地址的 POS 接口、配置 URPF 的 POS 接口；并且，POS 接口加入 HDLC 捆绑之后也不能配置这些功能。
- 成员接口加入 HDLC 捆绑前，请不要在该接口上配置三层业务（如 MPLS、VPN 等），如果成员接口上已有三层业务配置，请先取消该接口上所有的三层业务配置，再加入 HDLC 捆绑；加入 HDLC 捆绑后，相关业务也只能在 HDLC 捆绑接口上进行配置，如果在成员接口上误操作配置了三层业务，请先取消该成员接口上的所有三层业务配置，并在 HDLC 捆绑接口上执行 **shutdown**、**undo shutdown** 命令即可恢复。
- 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。
- HDLC 捆绑接口没有创建的情况下，也允许将接口加入 HDLC 捆绑。
- 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。
- 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。

表2-2 配置接口加入 HDLC 捆绑

操作	命令	说明
进入系统视图	**system-view**	-
进入POS接口视图	**interface pos** *interface-number*	-
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
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
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

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2-3 HDLC 链路捆绑显示和维护

操作	命令
显示HDLC捆绑信息（独立运行模式）	**display bundle hdlc-bundle** [*bundle-id*] **slot** *slot-number*
显示HDLC捆绑信息（IRF模式）	**display bundle hdlc-bundle** [*bundle-id*] **chassis** *chassis-number* **slot** *slot-number*
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*]]

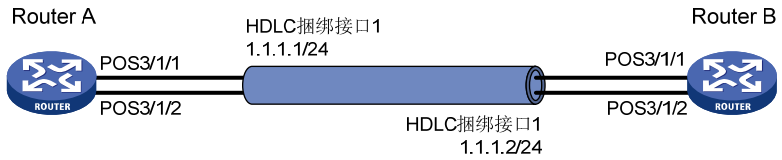
2.5 HDLC链路捆绑典型配置举例

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
```

(3) 验证配置结果

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 1
Bundle: HDLC-bundle1, slot 1
  max-active links: 8
  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

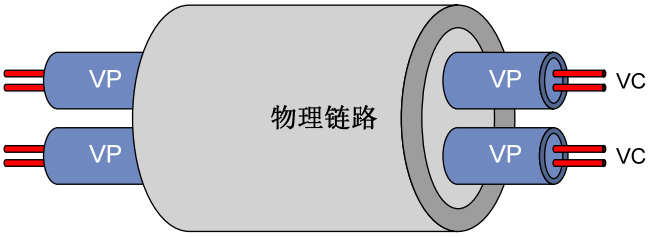
ATM（Asynchronous Transfer Mode，异步传输模式）技术是以分组传输模式为基础并融合了电路传输模式高速化的优点发展而成的，可以满足各种通信业务的需求。由于它的灵活性以及对多媒体业务的支持，被认为是实现宽带通信的核心技术。

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。

1.1.1 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。

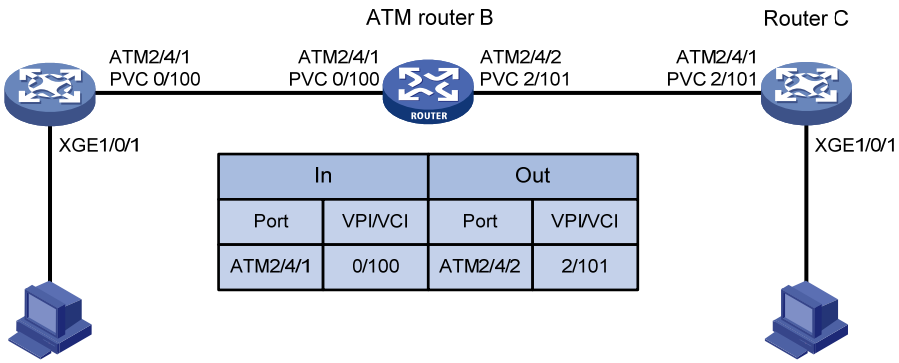
图1-1 VP、VC 和物理链路关系



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路由器的交换表项改变VPI/VCI值，实现ATM信元的转发。在PVC方式下，ATM路由器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路由器ATM router 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



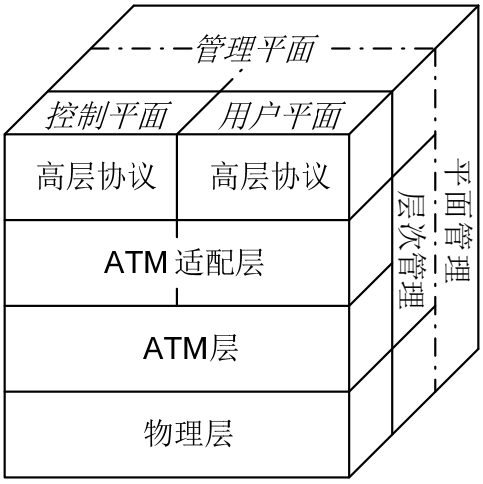
1.1.2 ATM层次结构

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、承载多种协议（IP 协议、IPoE 协议）等功能。

1.1.3 ATM服务类型

ATM 支持四种服务类型：

- CBR（Constant Bit Rate，恒定速率）
- UBR（Unspecified Bit Rate，非确定速率）
- 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 Cell，最大突发信元个数）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。

1.1.4 ATM应用

ATM 支持 IPoA 应用方式。

IPoA（IP over ATM）指的是在 ATM 上承载 IP 协议报文：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。

1.1.5 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 AIS/RDI（Alarm Indication Signal/Remote Defect Indication，告警指示信号/远程故障指示）告警信元检测：用户先指定相关参数，当收到指定数量 AIS/RDI 告警信元后，PVC 状态转变为 DOWN，当连续指定秒没有收到 AIS/RDI 告警信元后，PVC 状态转变为 UP。
- 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 配置限制和指导

仅 CMPE-1104 单板上的 ATM 接口子卡支持本功能。

1.3 ATM配置任务简介

表1-1 ATM 配置任务简介

配置任务	说明	详细配置
配置ATM接口	必选	1.4
配置PVC	必选	1.5
配置ATM的服务类型	必选	1.6
配置ATM上承载IPoA应用	必选	1.7
配置标记ATM信元的CLP标志位	可选	1.8
配置ATM OAM功能	可选	1.9

1.4 配置ATM接口

根据实际组网环境和系统运行的要求，有时可能需要改变 ATM 接口、ATM 子接口的某些参数。关于这些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”。

1.5 配置PVC

在 PVC 方式下，ATM 路由器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。

需要注意的是：

- ATM P2P 子接口只允许配置一个 PVC。
- 设备支持创建的 PVC 数量为 990。
- 当 ATM 接口/ATM 子接口下创建了两个或两个以上 PVC 时，该接口不支持使能 MPLS 能力（**mpls enable** 命令）、与交叉连接关联（**ac interface** 命令）、与指定 VPN 实例关联（**ip binding vpn-instance** 命令）。相关功能的详细介绍，请参见“MPLS 配置指导”中的“MPLS”、“MPLS L2VPN”和“MPLS L3VPN”。

表1-2 配置 PVC

操作	命令	说明
进入系统视图	**system-view**	-
进入ATM接口视图/ATM子接口视图	**interface atm** { *interface-number* | *interface-number.subnumber* }	-
创建PVC并进入PVC视图	**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }	缺省情况下，没有创建PVC
打开当前PVC	**undo shutdown**	缺省情况下，PVC处于打开状态

1.6 配置ATM的服务类型

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，并为 UBR、VBR-NRT、VBR-RT 服务类型的每条 PVC 配置不同的传输优先级，数值越大优先级越高。传输优先级高的 PVC 优先占有带宽，相同传输优先级的 PVC 占有相同的带宽。CBR 服务不允许配置传输优先级。

表1-3 配置 ATM 的服务类型

操作		命令	说明
进入系统视图		**system-view**	-
进入ATM接口视图/ATM子接口视图		**interface atm** { *interface-number* | *interface-number.subnumber* }	-
进入PVC视图		**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }	-
配置PVC的服务类型和相关服务参数	指定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*]	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
	指定PVC的服务类型为UBR，并指定相关的服务参数	**service ubr** *output-pcr*	
	指定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*	
	指定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*	

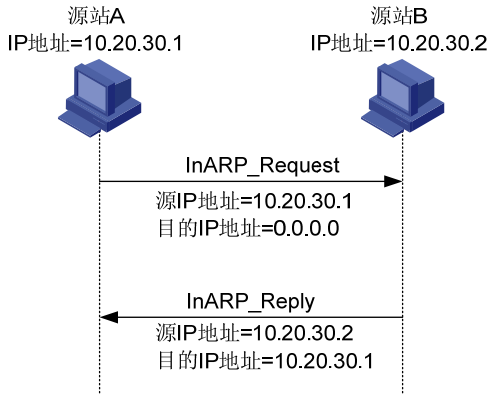
1.7 配置ATM上承载的IPoA应用

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 工作过程示意图



配置 IPoA 时需要注意：

- 同一 PVC 下只能映射一个 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。

表1-4 配置 IPoA

操作	命令	说明
进入系统视图	**system-view**	-
进入ATM接口视图/ATM子接口视图	**interface atm** { *interface-number* | *interface-number.subnumber* }	-
进入PVC视图	**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }	-
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，没有配置任何映射
（可选）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 如果在ATM PVC上需要发送广播或者组播报文，请务必配置此关键字

1.8 配置标记ATM信元的CLP标志位

用户可以通过设置 ATM 报文 CLP（Cell Loss Priority，信元丢失优先级）标志位的值，来重新定义 ATM 报文的丢弃优先级。下表中关于类、流行为、策略的详细介绍和相关配置，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

表1-5 配置标记 ATM 信元的 CLP 标志位

操作	命令	说明
进入系统视图	**system-view**	-
定义类并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	-

操作	命令	说明
定义匹配数据包的规则	**if-match** *match-criteria*	缺省情况下，没有定义匹配数据包的规则
退回系统视图	**quit**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
标记ATM信元的CLP标志位的值	**remark** [**green** | **red** | **yellow**] **atm-clp** *atm-clp-value*	缺省情况下，没有标记ATM信元的CLP标志位的值 ATM信元CLP标志位取值为0或1。发生拥塞时优先丢弃CLP为1的信元
退回系统视图	**quit**	-
定义策略并进入策略视图	**qos policy** *policy-name*	-
在策略中为类指定采用的流行为	**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为
退回系统视图	**quit**	-
进入ATM接口视图或者ATM子接口视图	**interface atm** { *interface-number* | *interface-number.subnumber* }	-
进入PVC视图	**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }	-
在PVC上应用关联的策略	**qos apply policy** *policy-name* **outbound**	缺省情况下，没有在PVC上应用QoS策略

1.9 配置ATM OAM功能

表1-6 配置 ATM OAM 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入ATM接口视图/ATM子接口视图	**interface atm** { *interface-number* | *interface-number.subnumber* }	-
进入PVC视图	**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }	-
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** *retry-interval*]	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
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**
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*]	本命令可以在任意视图下执行

1.10 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1-7 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* }]

1.11 ATM典型配置举例

1.11.1 IPoA典型配置举例

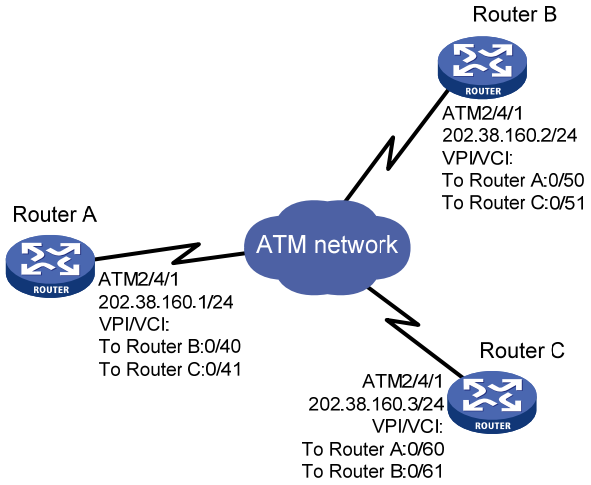
1. 组网需求

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。

1.12 ATM故障的诊断与排除

1.12.1 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。

1.12.2 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。

1.12.3 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。